Russia and Its Neighbours: Old Attitudes, New Capabilities

by

Keir Giles

Chapter 2 in
Kenneth Geers (Ed.), Cyber War in Perspective:
Russian Aggression against Ukraine,
NATO CCD COE Publications, Tallinn 2015

CCDCOE
NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

Cyber War in Perspective: Russian Aggression against Ukraine opens with a chapter by Russia scholar Keir Giles of the Conflict Studies Research Centre in Oxford, UK. Keir offers deep insight into the background to this crisis, and explains why it may not be resolved any time soon. Russia and the West are said to have two distinct views of the world. Moscow is unlikely to tolerate true independence and sovereignty for its former Soviet satellite states, and remains vehemently opposed to Western support for them. It has many strategies and tactics – traditional and cyber – that it can employ against Ukraine and its other neighbours, while the West is both hesitant and divided.

CCDCOE

NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

Disclaimer

This publication is a product of the NATO Cooperative Cyber Defence Centre of Excellence (the Centre). It does not necessarily reflect the policy or the opinion of the Centre or NATO. The Centre may not be held responsible for any loss or harm arising from the use of information contained in this publication and is not responsible for the content of the external sources, including external websites referenced in this publication. Digital or hard copies of this publication may be produced for internal use within NATO and for personal or educational use when for non-profit and non-commercial purpose, provided that copies bear a full citation. Please contact publications@ccdcoe.org with any further queries.

Chapter 2

Russia and Its Neighbours: Old Attitudes, New Capabilities

Keir Giles

Conflict Studies Research Centre

1 The View from Moscow

The crisis around Ukraine is part of a wider confrontation between Russia and the West, which has persisted at varying degrees of intensity since the fall of the Soviet Union despite periods when the West as a whole refused to recognise that any conflict of strategic interest with Russia existed. After a period where this confrontation lay relatively dormant, the conflict in Ukraine results from the culmination of two important trends in the Russian view of itself and the world: first, a greater and more urgent perception of threat, whether real or imagined, to Russia's own security; and second, a recognition that Russia itself has regained sufficient strength, military and otherwise, to assert itself.

The notion that Russia is faced with an existential threat – even when that threat is imperceptible from outside Russia – has multiple and complex origins. Some of these are permanent and persistent; for example, the idea of vulnerability of Russia's borders, which leads to the conviction that in order to protect its borders Russia must exert control far beyond them. In the last century this was one of the drivers for Soviet ultimatums to the Baltic states and Finland which eventually led to their invasion in 1939. This continuing perception feeds into the current portrayal by Russia of NATO enlargement, including to those same Baltic states, as a threat. Regardless of NATO's intent, it presents a menace simply by 'approaching Russia's borders'.[1]

[1] As expressed in a wide range of Russian security policy documents, including the December 2014 'Military Doctrine of the Russian Federation' and its predecessors.

Other, more recent developments have heightened the sense of urgency for Russian security planners. The fear that the West is considering bringing about regime change in Russia does not stand up to objective scrutiny, but appears deep-rooted among a broad sector of the Russian security elite. It has been accentuated in the past decade by, as Moscow sees it, further unrestrained and irresponsible interventions by the West with the intention of regime change, leaving chaos and disorder in their wake. Western action in Libya and support for anti-government rebels in Syria provide prime examples.

> *Recent developments have heightened the sense of urgency for Russian security planners.*

Thus the prospect of destabilisation closer to home in Ukraine would have been of even more acute and direct concern in Moscow. Even without the accompanying disorder, the threat of the 'loss' of Ukraine to the West posed an immediate military problem: it appears to have been considered plausible in Moscow that this presented an immediate danger of losing the Black Sea Fleet's base in Sevastopol, together with the often-overlooked supporting infrastructure scattered across the Crimean peninsula, to NATO. According to Secretary of the Russian Security Council Nikolay Patrushev, the consequences could be even more far-reaching: 'Americans are trying to involve the Russian Federation in interstate military conflict, to facilitate the change of power by way of using the events in Ukraine, and ultimately to carve up our country.'[2] Whether this view is sincerely held by the Russian leadership or not, it is the one that is consistently presented to the Russian public, and to its Armed Forces, as explaining the roots of the current conflict.

The fact that Russia was able to use large numbers of Special Operations Forces (SOF) swiftly and effectively to seize control of Crimea, and subsequently to wage an ongoing low-level campaign in eastern Ukraine involving long-term mobilisation of its conventional forces, is a pointer to the other key element of the new Russian approach to confrontation; the recognition that Russia is now in a position to exercise a much more assertive foreign policy than in the recent past.

One element of this is the unprecedented and expensive overhaul and rearmament of Russia's Armed Forces which began after the armed conflict with Georgia in 2008 and continues today. The fact that the Russian troops at work in Ukraine are entirely unrecognisable from the forces which entered Georgia just seven years earlier caused surprise and consternation among those Western defence communities that had not been paying attention. But the Ukraine campaign overall is far more than a military operation. Successful coordination of military movements and action with other measures in the political, economic and especially information domains, are the result of strenuous efforts by the

[2] Interview with Security Council Secretary Nikolay Patrushev, *Rossiyskaya gazeta*, 11 February 2015.

Putin administration over preceding years to harness other levers of state power to act in a coordinated manner.[3]

The results of this coordination has left the unprepared West scrambling for a response, and struggling even to define the phenomenon, as witness the tortuous attempts by NATO and Western governments to decide what precisely constitutes 'hybrid warfare'. But the notion of hybridity as applied to the current concept meets little understanding in Moscow. Instead, Russia can be said simply to be attempting to implement grand strategy in the classical sense. Russia's attempt at this whole of government approach to managing conflict is embodied in the National Defence Control Centre in central Moscow, where a wide range of different government ministries and agencies including those responsible for energy, the economy, ecology and more are brought together under the leadership of the General Staff.[4]

Intensive militarisation, sometimes referred to directly as mobilisation, is also now pervading Russian society, stoked by unending leadership rhetoric of war, confrontation and threat, and blanket military coverage on TV. According to Estonian Ambassador to the Russian Federation Jüri Luik, the Russian narrative of war is 'instrumentalising the population and putting it on a mental war footing', not only by tapping into the traditional Russian narrative of victimhood over centuries, but also by engendering 'a heroic feeling that now is the time of risk'.[5] Furthermore, analysis of Russian security thinking shows not only this asymmetry of threat perception, but also a complete divergence with the West in terms of notions of how and when the military should be used to counter those threats.

The notion of hybridity meets little understanding in Moscow.

As so often, there is no single explanation for a given course of action by Russia, and direct intervention in Crimea and Ukraine has also been parsed as a response to the threat posed to Russian business interests by closer integration with the European Union (EU). The EU model of open markets and rules-based dealings runs directly counter to the Russian way of doing business in the near abroad, reinforcing the growing Russian perception of the EU as a problem rather than an opportunity; but few analysts would have predicted that it would be the prospect of an EU Association Agreement for Ukraine, rather than any involvement with NATO, which would eventually lead to military intervention by Russia.

The ambivalent attitude to Ukraine as a sovereign nation with a right to choose its own foreign policy direction has its roots in an entirely different view of the end

[3] Andrew Monaghan. 'Defibrillating the Vertikal', Chatham House, October 2014, http://www.chathamhouse.org/publication/defibrillating-vertikal-putin-and-russian-grand-strategy.

[4] 'Начальник российского Генштаба рассказал журналистам о задачах и роли Национального центра по управлению обороной РФ', Russian Ministry of Defence website, 1 November 2014, http://function.mil.ru/news_page/country/more.htm?id=11998309@egNews.

[5] Speaking at the Lennart Meri Conference, Tallinn, 24 April 2015.

of the Soviet Union. That view holds that the former Soviet republics, including Ukraine and the Baltic States, in effect belong to Russia. According to President Putin, in 1991 'Russia voluntarily – I emphasise – voluntarily and consciously made absolutely historic concessions in giving up its own territory'.[6] This persistent view is not limited to President Putin. According to veteran scholar of Russia Paul Goble:

> *'The Russian elite is sincerely convinced that the preservation of influence on the former Soviet republics surrounding it is the status quo and a natural right given by history,' even though 'for the entire rest of the world such an approach is incomprehensible and unnatural'.*

What this means is that Moscow acts 'as if the Soviet Union had not fallen apart, as if it had only been reformatted, but relations between sovereign and vassal have remained as before'.[7] It is plain that at least in some sectors of society, these aspirations by Russia to regain imperial dominion over its surroundings enjoy broad support. The now-celebrated Prosecutor General of Crimea, Natalya Poklonskaya, in an interview at the time of annexation declared her ambition to 'start again in a great state, a great power, an *empire*, like Russia'.[8]

This approach to Russia's inheritance of domination over its neighbourhood appears consistent over time. In 1953, an assessment of recent history that had led to Soviet domination over Eastern Europe concluded that in the Russian view:

Informed analysis pointed to Ukraine as the next target for Russian action.

> *'Stalin was no more than reasserting Russian authority over territories which had long recognised Tsarist rule, and which had been torn away from Russia at the time of her revolutionary weakness after the First World War'.*[9]

The effect of these long-standing assumptions is a mind-set that leads to casual references by Russian generals to '*nashi byvshiye strany*' ('our former countries'), statements that even Finland and Poland were 'parts of Russia', and that all major powers have a non-threatening sanitary zone ('*sanitarnaya zona*') around them.[10] Russia's attempts to maintain, or reassert, this buffer zone are a major contributor to the current stand-off.

Since 1991, Moscow has employed a wide range of coercive tools in attempts –

[6] Ksenija Kirillova. 'Путин фактически назвал Украину территорией России', *Novyy Region 2*, 28 April 2015, http://nr2.com.ua/blogs/Ksenija_Kirillova/Putin-fakticheski-nazval-Ukrainu-territoriey-Rossii-95566.html.

[7] Paul A. Goble. 'Putin Gives the World His Geography Lesson: 'All the Former USSR is Russia'', *The Interpreter*, 28 April 2015, http://www.interpretermag.com/putingivestheworldhisgeographylessonalltheformerussrisrussia/.

[8] Russian television interview available at https://www.youtube.com/watch?v=XX4JCQViRKg (at 2'40").

[9] William Hardy McNeill. 'America, Britain and Russia: Their Co-operation and Conflict 1941-1946', (Oxford University Press 1953).

[10] Private conversations with author in late 2014.

often unsuccessful – to maintain influence and leverage over its Western neighbours.[11] From the mid-2000s, Russia benefited from a sudden influx of revenue thanks to higher oil prices and began to review its perception of its own strengths accordingly. From the earliest stages, this was reflected in huge budget increases for the Armed Forces,[12] and an intensified pattern of testing levers of influence against Western neighbours.[13] High-profile incidents during this stage included gas cut-offs for Ukraine in 2006, the crude cyber offensive against Estonia in May 2007, and ultimately the use of military force against Georgia in 2008. In each case, the results validated this approach for Russia: the Georgian conflict in particular demonstrated the validity of use of armed force as a foreign policy tool bringing swift and effective results, with only limited and temporary economic and reputational costs to bear.

It was in this context that a range of informed analysis pointed to Ukraine as the next target for assertive Russian action. A UK parliamentary report in 2009 noted that:

> *'Many of our witnesses stressed that Russia poses a military threat to other former Soviet states, particularly in light of its actions in Georgia... Some witnesses argued that Russia posed a military threat to Ukraine... one scenario was that Putin could send in military forces to secure the Russian military base at Sevastopol'.*[14]

2 Is This Cyber Warfare?

As noted above, the levers of power which Russia is bringing to bear in Ukraine are wide-ranging. This study looks in detail at the specific cyber conflict aspect of the Ukraine crisis, but even this concept is impressively broad thanks to the holistic and inclusive Russian approach to what constitutes information warfare, of which cyber is an integral part.

Opinions are divided as to whether what is taking place in and around Ukraine can or should be called cyber war. As Jan Stinissen argues in Chapter 14, current cyber operations do not meet a strict legal definition of a state of war. But at the same time, according to one analysis, operations in Ukraine undoubtedly constitute cyber warfare. The conflict:

> *'meets the generally accepted standard for the following reasons: the cyber warfare component is overt, meaning the perpetrators make little effort to hide either their identities or their allegiances. The two countries*

[11] For a recent overview of the unfriendly means Russia adopts to influence its neighbours, see 'Russia's Toolkit' in 'The Russian Challenge', Chatham House, June 2015, http://www.chathamhouse.org/publication/russian-challenge-authoritarian-nationalism.

[12] Keir Giles. 'Military Service in Russia: No New Model Army', Conflict Studies Research Centre, May 2007.

[13] Jakob Hedenskog and Robert L. Larsson. 'Russian Leverage on the CIS and the Baltic States', FOI, June 2007, available at www.foi.se/ReportFiles/foir_2280.pdf.

[14] 'Russia: a new confrontation?', House of Commons Defence Committee, Tenth Report of Session 2008-09, 10 July 2009.

> *are in open, hostile and declared conflict with each other. Both sides have stated military and political objectives'.*[15]

As if to emphasise the point, intensive cyber attacks reportedly cease during the occasional observance of ceasefires.[16]

Other elements of the cyber conflict also confound definition. Operations to date represent an evolution in Russian tactics compared to previous campaigns. Both cyber and traditional elements of conflict are present, but they are both less overt and more difficult to understand and defend against.

In part, this is due to Ukraine's very different cyber terrain. Comparisons to Russia's rudimentary cyber efforts at the time of the Georgian conflict in 2008 are of limited value. Unlike Georgia, Ukraine's more interconnected nature makes it impossible to restrict access to the internet overall, except in the very special case of the Crimean peninsula. But in addition, there is no reason why Russia should try, especially given the integrated nature of Ukrainian and Russian information space. Since Russia already enjoyed domination of Ukrainian cyberspace, including telecommunications companies, infrastructure, and overlapping networks, there was little incentive to disrupt it. In short, Russia had no need to attack that which it already owned.[17] To give one simplistic but indicative example, little offensive cyber effort is needed for Russia to access sensitive Ukrainian e-mail traffic when so many Ukrainians, including government officials, use Russian mail services and therefore provide automatic access to the Russian security and intelligence services.[18]

A distinctive aspect of information operations in Ukraine itself, and one with important implications for how cyber war may be waged in future, is the way Russian activity in the cyber domain facilitates broader information warfare aims. This manifests itself not only in straightforward spearphishing of Ukrainian officials[19] for exploitation, but also in specific uses of malware in the conflict.[20] A particular example is the redirection of malware originally intended for cybercrime to manipulating viewer figures to promote pro-Russian video clips.[21] But potentially even more significant for the nature of future cyber operations is the new interface

[15] Tony Martin-Vegue. 'Are we witnessing a cyber war between Russia and Ukraine? Don't blink – you might miss it', *CSO*, 24 April 2015, http://www.csoonline.com/article/2913743/cyber-attacks-espionage/are-we-witnessing-a-cyber-war-between-russia-and-ukraine-dont-blink-you-might-miss-it.html.

[16] Aarti Shahani. 'Report: To Aid Combat, Russia Wages Cyberwar Against Ukraine', *NPR*, 28 April 2015, http://www.npr.org/blogs/alltechconsidered/2015/04/28/402678116/report-to-aid-combat-russia-wages-cyberwar-against-ukraine.

[17] Patrick Tucker. 'Why Ukraine Has Already Lost The Cyberwar, Too', *Defense One*, 28 April 2014, http://www.defenseone.com/technology/2014/04/why-ukraine-has-already-lost-cyberwar-too/83350/print/.

[18] Anna Poludenko-Young. 'Ukrainian Officials, Russian Security Services Thank You for Your Cooperation!', *GlobalVoices*, 23 May 2015, http://globalvoicesonline.org/2015/05/23/ukrainian-officials-russian-security-services-thank-you-for-your-cooperation/.

[19] Undated PowerPoint presentation by SBU (Security Service of Ukraine), entitled 'В умовах військової агресії з боку Російської Федерації, війна ведеться не лише на землі, в повітрі та в дипломатичних колах, вперше в історії війн застосовані нові форми ведення агресії – гібридна війна з використанням кіберпростору України'.

[20] Kenneth Geers. 'Strategic Analysis: As Russia-Ukraine Conflict Continues, Malware Activity Rises', *FireEye*, 28 May 2014, https://www.fireeye.com/blog/threat-research/2014/05/strategic-analysis-as-russia-ukraine-conflict-continues-malware-activity-rises.html.

[21] Rami Kogan. 'Bedep trojan malware spread by the Angler exploit kit gets political', *Trustwave*, 29 April 2015, https://www.trustwave.com/Resources/SpiderLabs-Blog/Bedep-trojan-malware-spread-by-the-Angler-exploit-kit-gets-political/.

between cyber and kinetic operations. When Russia wished to isolate Crimea from news from the outside world, no sophisticated cyber exploits were required. Instead, SOF detachments simply took over the Simferopol IXP and selectively disrupted cable connections to the mainland.[22] In short, complex and expensive information weapons are entirely unnecessary in situations where the adversary can gain physical control of infrastructure.

> *Russian activity in the cyber domain facilitates broader information warfare aims.*

The circumstances of Crimea were unique, and not only because of the peninsula's distinctive internet geography; but Russian planners will have noted this striking success and will be looking for where it can be applied elsewhere. There are two important implications for planning for future crises with Russia. First, both civil and military contingency planning should include scenarios where friendly access to the internet is degraded or absent; and second, civilian internet infrastructure needs at least as much defence and protection as other strategic assets.

In any case, the course of the conflict so far has seen no visible full-scale cyber hostilities of the kind envisaged by theorists, a theme examined in more detail by Martin Libicki in Chapter 5. The tactics, techniques and procedures which have been used at various stages of the conflict are the subject of two separate detailed examinations by Nikolay Koval and Glib Pakharenko in Chapters 6 and 7.

3 Reactions and Responses

Information campaigning, facilitated by cyber activities, contributed powerfully to Russia's ability to prosecute operations against Ukraine in the early stages of the conflict with little coordinated opposition from the West. The fact that for almost a year the EU was unable to refer publicly to the presence of Russian troops in Ukraine[23] denotes a broader inability to challenge the Russian version of events without which a meaningful response is difficult or impossible. Early media coverage of the conflict made it 'apparent … that some interlocutors had swallowed whole some of the cruder falsifications of Russian propaganda'.[24]

As the realisation of the nature of the Russian information campaign began to filter through Western media and policy-making circles, this gave way to a dangerous optimism about the effectiveness of Russian measures, and a widespread assumption that Russian disinformation was failing because of its lack of plausibil-

[22] 'Кримські регіональні підрозділи ПАТ «Укртелеком» офіційно повідомляють про блокування невідомими декількох вузлів зв'язку на півострові', Ukrtelekom, 28 February 2014, http://www.ukrtelecom.ua/presscenter/news/official?id=120327.

[23] Andrew Rettman,. 'EU breaks taboo on 'Russian forces in Ukraine'', *EU Observer*, 16 February 2015, https://euobserver.com/foreign/127667.

[24] John Besemeres. 'Russian disinformation and Western misconceptions', *Inside Story*, 23 September 2014, http://insidestory.org.au/russian-disinformation-and-western-misconceptions.

ity. Supposedly, Russian lies were ineffective because they were so obvious that they did not confuse senior and intelligent individuals in the West. But this was to underestimate the effects of layered messaging, subtlety screened and concealed by more obvious fabrications, continued saturation, and in particular the pernicious effect of the 'filter bubble' on online reading habits – the way personalised search results driven by advertising models can effectively isolate internet users from alternative information and viewpoints.[25]

Russian official sources continue to disseminate lies which are easily detected and discredited in the West, as with the striking example of the 'discovery' of supposed US MANPADS in Donetsk in late July 2015.[26] But the implausibility is irrelevant for Russian objectives: the story has been planted and will continue to be disseminated via the internet, and will not be contradicted in mainstream sources within Russia. Instead of convincing Western readers that the disinformation is true, Russian success is defined in two other ways: isolating the domestic audience from non-approved information so that Russian state actions are permissible; and influencing foreign decision making by supplying polluted information, exploiting the fact that Western elected representatives receive and are sensitive to the same information flows as their voters. When Russian disinformation delivered in this manner is part of the framework for decisions, this constitutes success for Moscow, because a key element of the long-standing Soviet and Russian approach of reflexive control is in place.

> *Implausibility is irrelevant for Russian objectives.*

Crucially, it must be remembered that Russian disinformation campaigns aimed at the West are conducted not only in NATO languages, but also in Arabic and Russian targeting minorities across Europe. This itself has major implications for managing future confrontations between Russia and other front-line states, which must involve finding a means to respond to Russian information operations when the initiative necessarily lies with Russia. As put pithily by journalist and author Peter Pomerantsev, 'they will always win the narrative war, because they can make stuff up'.[27]

For the time being, much of the Western response appears focused on finding a label for the newly-demonstrated Russian way of warfare. A range of early contenders, such as 'non-linear war', 'ambiguous war' and others have largely been abandoned in favour of 'hybrid warfare', a concept originally designed for describing insurgency rather than warfighting by an aspiring regional power, but now applied to a totally new situation. Nevertheless many of the components now being used to define hybridity are nothing new in Russian practice. One argument

[25] 'How to Burst the 'Filter Bubble' that Protects Us from Opposing Views', *MIT Technology Review*, 29 November 2013, http://www.technologyreview.com/view/522111/how-to-burst-the-filter-bubble-that-protects-us-from-opposing-views/.

[26] Brian Ashcraft. 'Pro-Tip: Don't Copy Battlefield 3 Stingers', 23 July 2015, *Kotaku.com*, http://kotaku.com/pro-tip-dont-copy-battlefield-3-stingers-1719695507.

[27] Speaking at the Lennart Meri Conference, Tallinn. 24 April 2015.

holds that a previous round of expansionism by Russia in 1939-40 shared sufficient characteristics with current operations around Ukraine, including intimidation, spurious legitimation, and information campaigns backed with the prospect of full-scale invasion, to also be called hybrid warfare.[28] Russia's clinging to the attitudes and approaches of a former age holds other dangers too: Russian military, and in particular nuclear, messaging is baffling to its Western audience because the post-nationalist West has moved on from the Cold War mind-set in which it is rooted. The result is a dangerous situation where the messages from Russia are received, but not understood.

4 Outlook

At the time of writing the situation around Ukraine remains fluid and unpredictable. While Russia shows no signs of pushing for greater territorial control of Ukraine, moves toward conciliation by the West give rise to fears of appeasement and the danger of a repeat of the disastrous resolution to the Georgia conflict seven years before.[29] But one undeniable achievement by Russia is the transformation of the security environment in Central and Eastern Europe. Faced with a challenge that is no longer deniable, Europe has overcome its 'strategic inertia'.[30] NATO in particular has been revitalised: the NATO agenda has shifted radically from contemplation of a future role after withdrawal from Afghanistan, now that the Alliance has a clear motivation to return to its core purpose. Poland and the Baltic states, long cast as irresponsible trouble-makers for warning of the implications of a resurgent Russia, are now fully vindicated and benefiting from the overall NATO and unilateral US military response to the crisis. Each is at present supporting these front-line states with very small increments of conventional military forces, while considering how to respond to the broader threat of a more assertive Russia.[31]

The Ukraine conflict has the potential to bring about a transformative effect specifically within cyber doctrine. Unlike Russia, the siloed Western approach to cyber has typically focused on technical responses to technical threats, largely disregarding the interface with information warfare in the broad sense. This approach is entirely apt for persistent or background threats, but probably insufficient for when a national security crisis emerges, since at that point there will be no such thing as a 'pure cyber' confrontation. In other words, the West may have been well prepared

[28] Vitalii Usenko and Dmytro Usenko. 'Russian hybrid warfare: what are effects-based network operations and how to counteract them', *Euromaidan Press*, 17 January 2015, http://euromaidanpress.com/2015/01/17/russian-hybrid-warfare-what-are-effect-based-network-operations-and-how-to-counteract-them/.

[29] Karoun Demirjian. 'Visits by top U.S officials give Russia something to crow about', *The Washington Post*, 18 May 2015, http://www.washingtonpost.com/world/europe/visits-by-top-us-offi...about/2015/05/18/3c562a94-fd6b-11e4-8c77-bf274685e1df_story.html.

[30] Andrew A. Michta. 'Europe's Moment of Blinding Strategic Clarity', *The American Interest*, 24 October 2014, http://www.the-american-interest.com/2014/10/24/europes-moment-of-blinding-strategic-clarity/.

[31] Daniel Schearf. 'Russia Concerns Driving Neighbors to NATO', *Voice of America*, 5 August 2015, http://www.voanews.com/content/russia-concerns-driving-neighbors-to-nato/2903033.html.

for cyber war, but events in Ukraine show that it also needs to be prepared for information war when cyber operations are used as a facilitator or attack vector.

More broadly, Russia has clearly demonstrated an improved capability to coordinate its levers of state power in order to achieve strategic objectives in contrast to the West's apparent deficit of grand strategy. In his chapter 'Strategic Defence in Cyberspace: Beyond Tools and Tactics', Richard Bejtlich calls for strategic thought in cyber policy, but this approach needs to be mirrored across all domains in order to successfully counter the broad-based Russian approach to modern warfare.

The crisis around Ukraine has brought Europe closer to recognition that its values and interests are incompatible with those of Russia, and that if the West wishes to support Russia's neighbours in asserting their sovereignty and choosing their own destiny, confrontation with Russia is the inevitable result.[32] This also implies recognition that 2014–15 is not an aberration in relations between Russia and the West; rather, it is the previous 25 years of relative quiescence that were the exception to the rule. European nations have now been prompted by events to once more take an interest in their own defence. But while concentrating on countering and forestalling Russia's next unacceptable act of force, they must also be prepared for a sustained period of difficult and expensive tension.[33] In Russia's neighbourhood, the new normal is a return to old ways.

> *2014–15 is not an aberration in relations between Russia and the West.*

[32] A theme explored in greater detail in 'The Russian Challenge', op. cit.

[33] Keir Giles. 'Staring down a grizzly Russia', *The World Today*, Volume 70, Number 2, April–May 2014.