RUSSIAN
INTERNATIONAL
AFFAIRS COUNCIL

RUSI
www.rusi.org

REPORT

DEFINING DIALOGUE: HOW TO MANAGE RUSSIA–UK SECURITY RELATIONS. PART 2

38 / 2018

RUSSIAN INTERNATIONAL AFFAIRS COUNCIL

ROYAL UNITED SERVICES INSTITUTE

MOSCOW 2018

UDC 327.56(470:410)

Russian International Affairs Council
Royal United Services Institute

Defining Dialogue: How to Manage Russia–UK Security Relations. Part 2: Report No. 38/2018 / [A. Kortunov; M. Chalmers; S.Lain; M. Smekalova]; [I.S.Ivanov (Editor-in-Chief)]; Russian International Affairs Council (RIAC) and Royal United Services Institute for Defence and Security Studies (RUSI). – Moscow: NPMP RIAC, 2018. – 28 p. – The names of authors are listed on the reverse of the title page.

ISBN 978-5-6040387-7-2

At present, Russian-British relations are in a deep crisis. Will the countries be able to restore a regular and systematic dialogue at the highest level? What are the prospects for cooperation between Russia and Britain in military-to-military engagement, nuclear non-proliferation and cybersecurity? What mechanisms need to be worked out to strengthen confidence-building measures and develop cooperation in the fight against cybercrime? These and other issues related to the past, present and future of Russia–UK security relations are discussed in the joint report of the Russian International Affairs Council (RIAC) and the Royal United Services Institute for Defense and Security Studies (RUSI).

Cover photo credits:
up right: REUTERS/Dado Ruvic/Pixstream
left: REUTERS/KCNA/Pixstream

The full text is published on RIAC's website. You can download the report or leave a comment via this direct link – **russiancouncil.ru/en/report38**

TABLE OF CONTENTS

Introduction and Executive Summary

This report represents findings from the second round of the UK–Russia Track II bilateral security dialogue, held by RUSI in collaboration with the Moscow-based Russian International Affairs Council (RIAC). The dialogue, held between April and December 2017, brought together experts and former government officials from the two countries to discuss and debate ways in which the UK and Russia's bilateral security relationship can be better managed.

Initially conceived during a moment in relations when the United Kingdom and the Russian Federation appeared to be on a modestly upward trajectory, relations between the two countries worsened in March 2018 due to the poisoning with a nerve agent of Sergei Skripal and his daughter. The UK has laid the blame for the event on Moscow, and measures have been taken by both governments against each other. Our discussions were completed before these events, and therefore did not take them into account. Nevertheless, the project context remains strong, and the case for continuing dialogue between non-governmental experts is even stronger now that official relations between our two countries are tense and opportunities for dialogue at official level are becoming more limited.

The first round[1] explored an array of security and geopolitical topics to determine what areas of strengthened cooperation might be most fruitful. This second round focused on three of the most promising areas from the first round: military-to-military dialogue and risk reduction; nuclear arms control and nuclear threats, with particular reference to North Korea; and mitigation of common cyberthreats.

Although the discussion on all these topics raised difficult issues, the value of a Track II (that is, non-governmental) platform is that ideas can be brainstormed in an informal and non-politicised environment. In a bid to avoid unrealistic suggestions or discussions, RUSI and RIAC conducted private consultations with official interlocutors in London and Moscow prior to the three workshops and tried to involve as many experts with previous government experience as possible. This helped to balance creative thinking with suggestions grounded in political reality.

Military channels of communication were mostly cut following the 2014 Ukraine crisis, and it was agreed that this increased the risk of miscommunication or misunderstanding. While full restoration of previous levels of military dialogue remains unlikely in the current political environment, important opportunities for engagement do exist. From the UK side, these include proposals for the introduction of a crisis management hotline; the opportunity to follow up on the visit

[1] Sarah Lain and Andrey Kortunov, 'Defining Dialogue: How to Manage Russia–UK Security Relations', RUSI Conference Report, 28 March 2017.

to Moscow of the UK's Vice Chief of the Defence Staff General Gordon Messenger; and the potential to follow up on the UK's effort to be more transparent about what its armed forces are doing in Estonia and Poland as part of their contribution to NATO's Enhanced Forward Presence (EFP). Further small steps that could be taken might include deepening mutual access for UK and Russian defence attachés in Moscow and London respectively, and agreeing to provide more information about future military exercises. Russian experts did support the idea of a hotline, which may prove useful with regard to issues of both military-to-military engagement and cybersecurity. Special emphasis should be placed on cooperation between public and private entities in both countries as well as business-to-business contacts. Given the large number of British companies operating in Russia and vice versa, this opportunity must be utilised.

On nuclear arms control, there was general agreement that the ramifications of a breakdown in the existing Intermediate-Range Nuclear Forces (INF) Treaty and Strategic Arms Reduction Treaty (New START) agreements, which are both increasingly at risk, would have negative implications for both countries. Some UK participants highlighted the possibility that existing agreements may become increasingly obsolete as technology and military doctrine develops. It will also be increasingly important to give more attention to the growing potential for non-nuclear military technologies (including space, anti-missile and cyber capabilities) to have an impact on the correlation of nuclear forces. The potential for multilateralising such discussions, for example in the P5 nuclear dialogue, should be explored.

Regarding cybersecurity, participants from both countries identified a common interest among the commercial sectors in working together to counter cybercrime. This is more difficult at the government level, given that direct communication between law enforcement channels is difficult to achieve in the current political climate. However, it is still possible to communicate through other political channels or through third countries. The operation that took down the Avalanche criminal network shows how well cross-jurisdictional, private–public–not for profit cooperation can work. However, both the UK and Russia need to ensure that legislative frameworks are in place to allow for this kind of participation. Confidence and incentive still need to be built between private sector actors to ensure information is shared to combat crime, and national public–private sector trust needs to be enhanced. Public–private sector engagement has been controversial, with suspicions being aroused in the UK that private Russian cybersecurity firms may have links to, and may share information with, the security services. Even if this is the case, it does not preclude all dialogue with private sector stakeholders.

Overall, it must be borne in mind that all expectations for bilateral cooperation in these highly sensitive – in terms of national security – areas should be managed against the background of the current state of the West–Russia relationship, which is a function of the broader evolution of this relationship over the post-Cold War period. Those issues are subject to collective positions within the Western alliance, whether that is NATO, the EU, or the US–UK special rela-

tionship. For example, according to some Russian experts, the British military deployment in the Baltic states is part of the NATO project, which is why, as it turned out, there could be no bilateral arrangement on prevention of incidents in the air along the lines suggested by Finland in the summer of 2016 (see footnote 11 in this Chapter). It is clear that US President Donald Trump's policies will have an impact on the political landscape in these areas, based on the administration's first National Security Strategy, National Defense Strategy and Nuclear Posture Review, adopted between December 2017 and February 2018.

UK participants expressed concern that increased Russian 'information warfare', including well-organised alleged attempts by Russian-based organisations to interfere in political processes in the West, are undermining mutual trust, and make it more difficult to build confidence in other areas. In contrast, Russian participants noted that the politicisation of information, misinformation coming from numerous outlets, and interpretation versus information conflict further undermine trust between Russia and the West, making cooperation on matters of shared interest more challenging. Participants from both countries agreed that every effort must be made to keep those problems from contributing to a further worsening of West–Russia relations, both at inter-governmental and societal levels.

Military–to–Military Engagement

The first session of the 2017–2018 RUSI–RIAC Track II security dialogue, held in London in October 2017, built on an issue identified in the previous discussions as worthy of further exploration. Previous discussions noted that severing the military–to–military dialogue potentially caused problems in bilateral risk management and increased the likelihood of misunderstanding and miscalculation. This discussion focused on identifying further steps that could be taken to enhance UK–Russia military or security engagement.

Recommendations

- Meaningful engagement on military matters will likely be achieved through taking small steps on transparency, risk reduction and improved communication. This should be the focus for UK–Russia relations in the short-term rather than bigger issues, such as new confidence-building agreements or creating a new security architecture. Brainstorming the key obstacles in arms control, confidence-building measures and security architecture is still useful, as it can help unlock ideas for small concrete measures and enhance mutual understanding. However, it will likely be a longer-term exercise given low levels of trust.
- More could be done on transparency over large-scale military exercises. Provision of meaningful information will help to reassure both sides that there are no hidden intentions behind them. It was noted that the UK was more forthcoming than previously on its activities in NATO's EFP, but it had been disappointed that Russia did not offer the same transparency on its *Zapad 2017* military exercises.
- The UK and Russia should seek areas of military-to-military cooperation that are not politically motivated, but perhaps relate to safety and humanitarian issues, such as submarine search and rescue and disaster relief.
- It was suggested that the success of the Incidents at Sea (INCSEA) agreement could be used to create an 'Incidents in the Air' agreement to try to prevent dangerous manoeuvres.
- Institutional knowledge on confidence-building and arms control, both conventional and nuclear, should be reinvigorated. Participants noted their concern that knowledge on these topics is waning, particularly among younger generations.

The Difficulties of Confidence-Building

Realistic attempts at military dialogue will initially require relatively small steps aimed at specific objectives, such as risk reduction and information sharing. Large confidence-building initiatives are difficult to envisage given the low level of trust, let alone the formulation of new formal agreements on, for example,

conventional arms control. Instead, crisis prevention should be the focus of bilateral military and security discussions. As one UK participant noted, there seems to be a 'mutually assured misperception' on both sides. Regardless of political disagreements, the bilateral relationship still needs to be managed.

Ambiguity in existing conventional, and indeed nuclear, agreements, such as the Vienna Document 1990 (as subsequently updated)[2], the 1987 INF Treaty between the US and Russia[3], and the 2002 Open Skies Treaty[4] is being exploited for political gain, which undermines the objective of existing confidence-building measures. For example, although Russia announced that 12,700 troops would be participating in the *Zapad 2017* exercises in Belarus last September, which is below the 13,000-threshold requiring observation according to the Vienna Document, there were many other official exercises taking place in Russia itself simultaneously that were not classified as part of *Zapad*. The Russian experts noted that this was when huge exercises usually took place in every military district. However, the delineation was not clear, in NATO's view, and could be interpreted as exercises on a much larger scale.

Amendments to agreements, although much needed, are unlikely to be agreed on in the current environment. Even this topic itself has become a source of dispute. Russia would argue that it had previously proposed reforming and updating, for example, the Vienna Document, but that the West did not engage. Now the West would like to consider this, and it is Russia's turn to decline.

Part of this growing challenge is that aspects of existing agreements, even when there has been the trust needed to make them work in spirit and practice, are becoming obsolete. The current dynamic of military modernisation and warfare does not relate as much to numbers of weapons as to mobility, firepower and capability. Moreover, states not previously covered by agreements are emerging as modernised military powers. Countries are increasingly aware of the competitive advantage of not being part of conventional arms control agreements or confidence-building measures.

Looking to the future, participants noted a concern that the legal, ethical or administrative framework for new technology and its role in the military (for example, autonomous weapons or artificial intelligence) is not developing swiftly enough. In the current political environment, agreement on limits or rules regarding new technology may be difficult to reach. Despite this, participants expressed their hope that the broad frameworks and motivation behind previous confidence-building measures would make all sides aware of the dangers of failing to think ahead as technology develops.

One specific concern that was raised when discussing confidence-building measures and arms control, both conventional and nuclear, was that institutional knowledge is waning on why they are needed. As younger generations tend not to study such issues, this should be encouraged.

[2] OSCE, 'Vienna Document 2011 on Confidence and Security-Building Measures', 30 November 2011.
[3] Arms Control Association, 'The Intermediate-Range Nuclear Forces (INF) Treaty at a Glance', 22 December 2017.
[4] OSCE, 'Open Skies Consultative Commission', <http://www.osce.org/oscc>, accessed 18 February 2018. The Treaty on Open Skies currently has 34 members, drawn from OSCE member states.

Military-to-Military Engagement

At the bilateral level, it was agreed that tensions between Russia and the UK existed long before events in Ukraine, which is not to say that security and military cooperation did not exist. For example, in January 2014 the UK Ministry of Defence (MoD) and the Russian Federal Service for Military Technical Cooperation were planning to sign a Military Technical Cooperation Agreement.[5] However, developments in Ukraine, particularly Crimea in March 2014, resulted in a new low in relations and halted most cooperative activities in the military space.

As a result, military-to-military cooperation, and communication to a large degree, was severed. Restoring cooperative measures is not feasible in the current climate. However, it was noted that engagement is desirable on both sides where there is specific purpose and potential to produce concrete results. This is particularly relevant in the realm of risk reduction and transparency.

There have been some successes in maintaining certain existing bilateral initiatives, despite heightened tensions. For example, everyone agreed that the incidents at sea (INCSEA) process works well, with updates to the process being agreed on in 2017. A suggestion was made to expand on some of the successes of this initiative by creating an 'incidents in air' agreement, modelled on INCSEA, to tackle dangerous manoeuvres. There was also a meeting of Russian and UK hydrographers in St Petersburg in 2017, the first in ten years. Although encouraging, these initiatives are not sufficient alone to address the risks of miscalculation and misunderstanding that exist between the two countries.

Direct bilateral engagement needs to be strengthened, if only as a communication channel. Over the past eighteen months, the UK has stepped up its efforts to engage the Russian military. For example, a hotline for crisis and incident management between the MoD and Russia's National Defence Management Centre was established after the UK's then VCDS Air Chief Marshal Sir Stuart Peach visited Moscow in December 2015.[6] This visit was followed up in February 2017 by the new VCDS, General Sir Gordon Messenger, who met his opposite number Colonel General Alexander Zhuravlyov. Peter Watkins, the director general security policy in the Ministry of Defence, met Russia's deputy minister of defence Alexander Fomin on the sidelines of the Shangri-La Dialogue, a Track I inter-governmental security forum held annually by the International Institute for Strategic Studies, attended by defence ministers, permanent heads of ministries and military chiefs of 28 Asia-Pacific states.[7]

During the VCDS's visit to Moscow in February 2017, the UK was also more forward-leaning in discussing transparency with Russia, presenting what it believed to be new information on the UK's contributions to the NATO EFP in Eastern Europe. Although Russia also presented information on the *Zapad* exercises, UK participants felt that the information given was too broad and

[5] Matthew Holehouse, 'Comrades in Arms: Britain and Russia to Sign Defence Deal', *The Telegraph*, 26 January 2014.
[6] Author interview with UK MoD representatives, London, July 2017.
[7] *Ibid*

generalised. Transparency over large-scale exercises presents a future opportunity for bilateral engagement.

Therefore, the perception that the UK was at the 'back of the pack' on confidence-building measures, as suggested in the last RUSI–RIAC report, was viewed by one expert as misleading. There was a sense that the UK has tried but cannot move forward until Russia reciprocates. Suggestions on how this could potentially happen are made below.

More information about the *Zapad* exercises could have been provided as a goodwill gesture, particularly given that similar events held previously have preceded Russian-backed campaigns in Georgia and Ukraine. One Russian expert suggested that Russia could have gone up to the 13,000 personnel Vienna Document threshold for *Zapad*, to trigger inspections and to prove it had nothing to hide. Although this may not appeal to the Russian government, such ideas are useful in determining how – when there is the political will – confidence-building measures might begin to be restored. For its part, as it prepares for its own future military exercises in Europe, it will be important that NATO continues to meet its Vienna Document obligations.

Regarding military-to-military contacts, it would be highly useful to sustain some current UK–Russia engagements. Zhuravlyov is now commander of the Eastern Military District, and it is not clear who will replace him. His successor will be crucial for continuing the UK–Russia military-to-military dialogue. One UK expert also suggested that military-to-military dialogue could be enhanced at the operational level, for example between the UK Chief of Joint Operations and Russia's Western Military District Commander.

Generally, it was noted that there are very few personal working relationships among senior serving military officers, or even ministers relevant to defence and security, between Russia and the UK. Therefore, expanding some of these contacts to facilitate clearer communication will be useful, even while political tensions remain high. However, ad hoc meetings are not enough and there should be an established pattern of contact. This will work best if coordinated closely with the UK Foreign and Commonwealth Office and the Russian Ministry of Foreign Affairs, as highlighted by Foreign Secretary Boris Johnson's visit to Moscow in December 2017.

Lessons could also be learnt regarding the architecture of sanctions and their impact on engagement. One UK participant highlighted that military-to-military communication, which was crucial at the height of the Ukraine crisis, suffered mainly due to some tactical errors in the sanctioning of some of Russia's military leadership. For example, at the time, Peach had a good working relationship with then first deputy minister of defence, Arkady Bakhin. This would have been a useful communication channel had Bakhin not been sanctioned, which curtailed this option.

There are still potentially non-controversial, and previously successful, areas that could be explored for engagement, such as submarine search and rescue.

The UK provided a rescue team to help the crew of the AS28 deep-submergence rescue vehicle in the Pacific Ocean in 2005. President Vladimir Putin subsequently awarded the British team the Order of Friendship.[8] Disaster relief is another area where there may be some constructive dialogue with small, but concrete, outcomes.

Formats for Further Engagement

At the more multilateral level, the discussion addressed other formats for engagement beyond bilateralism. Many felt that there has been an over-emphasis on what role multilateral organisations could have played in the past to manage crises. For example, some participants criticised the NATO–Russia Council (NRC) for failing to de-escalate the situation in Ukraine. Although this could have been a useful forum for dialogue as the situation unravelled, it would still have been hindered by the seemingly irreconcilable approaches to security that NATO and Russia advocate. On the one hand, NATO's eastward expansion is a concern for Russia; and on the other, NATO will not change its open-door policy to suit Russia. Moscow couches NATO's EFP in terms of provocation, but to the Alliance it is clearly a response to Russia's actions in Ukraine.

This is not to say that the NRC is a fruitless platform, but it needs to redefine its goals to counteract an increasing divergence of approaches to security. Reforming and revitalising the NRC working groups could help to focus this. The NATO–Russia relationship is a source of great difficulty, but will continue to be so if communication is not improved. Approaching the relationship from a new angle might mean considering a dialogue between NATO and the Collective Security Treaty Organisation (CSTO). Although there has been reluctance to consider this on the part of NATO, more creative thinking is required at least to try to reinvigorate formats.

Even when initiatives are suggested, the deep suspicion between NATO member states and Russia prevents meaningful progress. For example, when Russia proposed discussions on security, including air safety measures, with the Baltic states, Poland, Sweden and Finland in August 2016,[9] Lithuania and Estonia rejected the offer for fear that this initiative was really aimed at dividing NATO unity. Russia could then use this as an example of how NATO countries are uncooperative when it comes to addressing security concerns. This problematic approach and response, and rebuff by NATO states of any initiative without further engagement, is a repeated theme in discussions on European security.

Part of the broader complaint from Russia is that the current European security architecture, dominated by NATO, excludes Russia itself. NATO and Russia have managed to forge constructive bilateral relations previously, with Russia's joining the North Atlantic Cooperation Council in 1991 and the launch of the Partnership for Peace programme in 1994, but this has not been sufficient. A key

[8] 'Putin Honours Submarine Rescue Team', *The Guardian*, 5 October 2005.
[9] Justyna Gotkowska and Piotr Szymański, 'Russia's "Niinistö Plan"', The Centre for Eastern Studies, 25 August 2016.

challenge in addressing this problem is that many European states have views on regional security architecture that differ from Russia's. Therefore, adaptation on a more inclusive level that takes all Russia's interests into account would be difficult due to Moscow's approach to countries such as Georgia and Ukraine. Still, Russian experts increasingly believe that a resolution to the Ukraine crisis cannot be found strictly within the framework of making the present 'patchwork' of European security architecture truly inclusive. The situation could be deemed a function of the choice made by the West in the 1990s in favour of hedging against Russia through NATO expansion rather than building a binding, norm-based and inclusive formal post-Cold War settlement.

In the absence of a security architecture that works for both Russia and NATO, some Russian experts point to the OSCE as a space where security dialogue could be strengthened. However, this organisation has not developed into a regional security organisation as per Chapter 8 of the UN Charter. Although the structured dialogue process and capability mapping exercises taking place at the OSCE are highly valuable in reinvigorating debate over the structure and substance of confidence-building measures, its impact and implementation of any concrete agreement will likely be limited. The OSCE suffers from a somewhat limited mandate and can be hindered also by the number of often contrasting interests its various members have. This is something from which any multilateral organisation suffers. The OSCE still provides a highly useful platform, but there are clearly limitations that should be recognised.

Therefore, in the absence of any formal agreement on a workably inclusive security architecture in the short term, more concrete steps can be taken at the bilateral level. Continuing dialogue in broader multilateral security formats, such as the OSCE and the NATO–Russia Council, is still vital, and creative thinking about their reform is useful. Bilateral initiatives can also help to provide stimulus for such thinking.

Nuclear Arms Control

The second RUSI–RIAC bilateral security dialogue workshop took place in Moscow in November 2017, gathering experts to discuss the future of nuclear arms control and broader nuclear threats. The geopolitical case study of North Korea was explored as a shared potential bilateral challenge. Although nuclear arms control itself is principally a US–Russia bilateral issue, the ramifications of this relationship breaking down are highly pertinent for the UK and Europe. Furthermore, Russia often views US capability as supplemented by NATO capability, and the territory of the Alliance's member states as a US strategic territory, used for 'a resilient forward posture'.[10] Given that the UK is a P5 country, a NATO member and a nuclear power itself, it was still deemed a relevant topic to explore.

Recommendations

- Arms control has traditionally been a US–Russia issue. However, this may now be an outdated, or at least insufficient, framework. Wider discussions might also usefully take place in the P5 nuclear process. Although there may be little appetite to multilateralise arms control, more dialogue on the issue is required.
- Although speculation about the role of new and future technology and its impact on arms control is challenging and not necessarily always useful, it could form a basis for exploring what the implications will be for existing nuclear arms control. There are already new arenas for warfare that could link to nuclear weapons, such as space, as well as new types of weapons, including hypersonic, underwater and autonomous weapons, and rapidly developing types of warfare, for instance cyber and electronic. This raises the prospect of asymmetrical responses that may involve nuclear weapons.
- With new technology, the determinants of strategic stability are changing. Given the risk of erosion and abandonment of nuclear arms treaties, further analysing what calculations factor into political thinking on strategic stability is required for more short-term responses for conflict prevention.
- The threat of a nuclear North Korea is a common concern for Russia and the UK. However, it is not clear how policies may align on this issue in practice. The UK acknowledges that, although China is a dominant player when it comes to North Korea, Russia tends to have expertise on, and good access to, North Korea, and therefore can be a valuable interlocutor. Enhanced sharing of expertise and information at the expert level could be a good first step in this regard.

When discussing arms control, it was noted that the INF and, in turn, New START treaties are in danger of collapse. If either side withdraws from the INF, it

[10] The White House, 'National Security Strategy of the United States of America', December 2017.

is unlikely that discussions on the extension of New START, due to expire in February 2021, will progress. If these negotiations collapse, it could also have negative consequences for the Nuclear Non-Proliferation Treaty (NPT) Review Conference in 2020.

The tension over INF comes from accusations of violations. The US has raised concerns that Russia has deployed a ground-launched cruise missile (the Novator 9M729) with a range capability of 500–5,500 kilometres, in violation of the INF. This is a long-standing issue, with tests of this missile beginning in 2008.[11] Concerns were raised at a meeting of the Special Verification Commission in November 2016, but there was no progress in resolving these concerns.[12]

Russia has accused the US of violating the treaty by deploying the Mark 41 Vertical Launch System (VLS) – a component of a missile defence system that Russia says could be modified to launch offensive cruise missiles. It also claims that some US armed drones are effectively banned cruise missiles, and that the US further violates the agreement by using intermediate-range missiles as targets during missile defence system testing.[13]

There was some discussion over whether it would be productive to introduce a simple arrangement for inspections over two of the key sticking points around nuclear arms control – that is, the 9M729 ground-launched cruise missile that Russia has developed and tested, and the US Mark 41 Vertical Launch System for Aegis Ashore, now being deployed in Poland and Romania. Tactical nuclear weapons could be another area warranting more specific discussion in relation to arms control. However, with mutual trust being so low at present, it is unclear how feasible any agreement would be.

There is also a divergence in protocol for expressing grievances. One Russian expert noted that Moscow's preference is to act within existing channels on arms control, whereas its perception is that the US prefers to act outside them. In the case of INF, they argued, concerns should be presented within the INF Special Verification Commission, rather than what Moscow views as the US using public forums to hint at Russian defection from it.

New leadership in the US, including the accompanying rhetoric, has also added to uncertainty over American commitment to nuclear arms control. Although the modernisation of the US nuclear arsenal was proposed under the Obama administration, Trump has pledged to make the nation's nuclear deterrent 'far stronger and more powerful than ever before'.[14] The recently published US Nuclear Posture Review[15] directly addresses Russia on a number of issues. It notes the intention to build up more low-yield nuclear options to enhance deterrence; to develop an 'arms control compliant' sea-launched cruise missile to respond to the perceived Russian violation of the INF; and considers using a nuclear response

[11] Amy F Woolf, 'Russian Compliance with the Intermediate Range Nuclear Forces (INF) Treaty: Background and Issues for Congress', Congressional Research Service, 6 December 2017.
[12] *Ibid*
[13] Ankit Panda, 'The Uncertain Future of the INF Treaty', Council on Foreign Relations, 21 December 2017.
[14] Gregory Hellman, 'Trillion-Dollar Nuclear Arms Plan Sets up Budget Brawl', *Politico*, 31 October 2017.
[15] US Department of Defense, 'Nuclear Posture Review', February 2018.

to react to a serious non-nuclear strike on, for example, US infrastructure.[16] The US defence policy bill from November 2017 set aside $58 million to respond to Russia's perceived INF violation, including research and development funds for its own intermediate-range missile.[17]

Putin has said Moscow remains committed to the INF but has warned about Russia's response should the US withdraw, almost pre-emptively blaming the US for the agreement's collapse. In his Valdai speech in October 2017, Putin referred to the INF Treaty, saying 'If someone does not like it [the INF treaty] and wishes to withdraw from the treaty, for example, our American partners, our response would be immediate, I would like to repeat this warning. Immediate and reciprocal'.[18]

Apart from rhetoric and policy that appears as if it may be moving away from arms control, an added difficulty with Cold War-era nuclear arms control agreements is that as bilateral agreements, they are more difficult to maintain as other countries develop their own nuclear capabilities. Multilateralising agreements has been proposed, but there is significant doubt as to how much political appetite there would be from countries such as China to agree to reductions or controls. Even having bilateral agreements between nuclear states other than the US and Russia seems difficult. However, this is still something that could be brainstormed further at a Track II level to bring in a P5 dimension to discussions.

As mentioned regarding conventional arms control, all sides expressed concern about the erosion of institutional knowledge on nuclear arms control. A potential starting point for enhancing the rectificaton of this may be conducting joint Russia–UK studies on the ecological and climate impacts of nuclear weapons use for Europe, building on the 'nuclear winter' hypothesis.

New Technology

Moreover, technology is changing the landscape of conventional, nuclear and non-conventional capabilities that have an impact on nuclear arms control agreements. New technologies raise the prospect of potentially purposeful or even 'inadvertent nuclear use' in Europe, particularly as an option for asymmetrical responses, as suggested by the leaked US Nuclear Posture Review document. Brainstorming some scenarios for mechanisms to contain new joint threats could be useful in also brainstorming ways to handle current threats.

These evolving tools and weapons affect the security of nuclear delivery systems. The potential, for example, for terrorists to use cyber capabilities to take control of nuclear weapons systems means the question of nuclear arms control is still relevant, but it is facing new threats that concern all powers. Hacking of state nuclear facilities by other states actors is also of increasing concern.

[16] Aaron Mehta, 'Nuclear Posture Review Draft Leaks; New Weapons Coming Amid Strategic Shift', *DefenseNews*, 12 January 2018.
[17] Steven Pifer, 'Order from Chaos: U.S. Response to Russian Treaty Violation Plays into Moscow's Hands', Brookings Institution, 15 November 2017.
[18] President of Russia, 'Meeting of the Valdai International Discussion Club', 19 October 2017.

On space, one UK participant noted that there was at least one positive from this development, given that it provided a wider range of verification methods. For example, if India conducted nuclear testing, it would likely be noticed given that there are 'so many eyes in space'. They suggested that the principles of Cold War-era arms control agreements, which look increasingly 'anachronistic', could still be used as a model to discuss rules and verification on new technology to try to anticipate new challenges.

There has been some thinking on this concerning space. For example, in 2014, Russia and China submitted an updated draft of their Treaty on the Prevention of the Placement of Weapons in Outer Space. The US has rejected this on numerous grounds, key ones being a lack of a verification mechanism as well as an absence of restrictions on the development of anti-satellite weapons on the ground.[19] As one UK participant noted, the technical details are too broad to be implemented in the proposal, but it is at least the start of a dialogue on conflict prevention. Still, given the political climate, it is difficult to envisage agreement on this, but it is a conversation that is needed to pre-empt conflict in rapidly developing areas.

This indicates that the idea of strategic stability is also changing. Given the risk of erosion and abandonment of nuclear arms treaties, further analysing what calculations factor into political thinking on strategic stability is required for more short-term responses for conflict prevention.

North Korea

The group discussion specifically examined the threat from North Korea and how this might be a shared interest between Russia and the UK. A nuclear North Korea seems to be a common concern for both countries. However, one difficulty is determining how much of a joint response there can be on this. UN sanctions have been agreed, but it has been noted that there are Russia-based individuals and companies in violation of the sanctions. Therefore, from a policy perspective, methods for responding to North Korea may not fully align, but there may be more specific concerns that could form the basis of a dialogue. These include the prevention of the onward sale of weapons or capabilities developed by North Korea.

There is again a sense that proposals or agreements may be used to undermine the process, rather than to genuinely find a constructive way forward. For example, the Russia–China 'freeze-for-freeze' suggestion, as presented, seems disingenuous to the UK audience. It is a non-starter that South Korea and the US would cease exercises, and the West would expect Russia to know this. Despite this, it is certainly worth having further talks based on the suggestion. For there are no other proposals to achieve the shared goal of a denuclearised Korean Peninsula.

[19] Jeff Foust, 'U.S. Dismisses Space Weapons Treaty Proposal as "Fundamentally Flawed"', *SpaceNews*, 11 September 2014.

Most agreed that disarmament is not a feasible short term aim when it comes to North Korea, given how developed Pyongyang's nuclear programme has become. Thus, the world will likely have to engage with Pyongyang as a de facto nuclear state. A key risk is that North Korea's level of expertise and analysis on other states can be poor, and vice versa regarding some Western countries. For example, one Russian expert noted that Pyongyang's expertise on US policy-making processes is very weak. This potentially increases the risk of miscalculation.

Although China is often seen as the main associate of Pyongyang, it was noted that Moscow tends to have good political access in North Korea as well. One UK participant noted that in many ways the UK acknowledges this, in contrast to the policy of the US. Furthermore, the UK is one of the few countries that has a diplomatic presence in Pyongyang. This shared interest in trying to engage Pyongyang could form a foundation for Russia and the UK to share expertise.

That is not to say that either Russia or the UK is influential on North Korea, given that China is the main foreign power with leverage. However, both the UK and Russia would like to see the stabilisation of the Korean Peninsula. Russia is interested in seeing economic and energy projects implemented, such as a planned gas pipeline through North Korea. Moreover, there is certainly room for other powers to try to be more involved, given clear scepticism that China will do anything other than implementing sanctions to try to rein in Pyongyang. North Korea itself is seeking a more independent policy from China as Kim Jong-un changes his leadership style.

Cybersecurity: Potential for Common Ground?

With cyber/information security rapidly becoming a priority area for government and the private sector, countries are seeking to be proactive when it comes to defining their policies and combating cyberattacks. As with many security issues relevant to the Russia–UK relationship, 'cyber' has been strongly influenced by politics. Last year hostility followed from accusations that Russia had used cyber proxies to interfere in elections in the US and Europe. Although the resulting political tension means that any agreement over rules of engagement in cyberspace appears highly unlikely in the short term, it does provide a new impetus for expert engagement on key challenges in the broader cyber debate. These include threat perception, attribution of cyberattacks and legal-technical barriers to cooperation on shared interests, such as cybercrime.

There is currently little trust at the political level. However, the third RUSI–RIAC workshop in this series brought together experts from the private sector and academia as well as former government officials. This enabled people to understand different perspectives on cyber threats and explore ways in which the private sector specifically might have a more constructive relationship on countering such threats.

Recommendations

- Although discussions on norms in cyberspace have so far produced few concrete agreements, they are useful for understanding how countries view the challenges and threats. Still, expectations must be managed as to what such discussions will be able to achieve. Given the usefulness of cyber tools for states and the difficulty in finding common definitions of defensive, deterrent and offensive activity, as well as determining attribution, norms are unlikely to be agreed on, let alone enforced.
- At the government level, a UK–Russia cyber hotline for reporting criminal activity could be a logical initiative, particularly due to the 2018 FIFA World Cup being held in Russia this summer. Information sharing between law enforcement in the UK and Russia is challenging for political and security reasons, but there are still methods for cooperation where there is a shared threat, either through non-law enforcement political channels or third countries.
- The operation that led to the dismantling of the Avalanche criminal platform is a prime example of how cooperation between multi-jurisdictional public, private and not-for-profit sector actors can and should work. This benefited from partnership between law enforcement agencies of multiple countries; multilateral law enforcement organisations such as Europol; the private

sector; and non-profit organisations, such as Russia's Coordination Centre for Top Level Domains (CCTLD), an organisation that administrates the domains .ru and .rf, ICANN and Shadowserver. Although this took many years and resources, it highlighted the benefits of a multilateral approach to combating crime.

- Streamlining the legal process for sharing information would be beneficial to both parties. Russia and the UK are both signatories to the European convention on mutual assistance on criminal matters, signed in 1959. What is more, the parties signed the Memorandum of Understanding between Public Prosecution Service of the Russian Federation and Crown Prosecution Service. These existing frameworks may and should be used when investigating and prosecuting cybercrime. Even though using legal instruments may prove cumbersome and time-consuming, they lay solid ground for bilateral efforts on fighting cybercrime and resolving existing issues.
- Exploring other formats and modalities for meaningful cooperation between public and private sectors at the national and international level was also recommended. At the more inter-state level, it was suggested that Computer Emergency Response Teams (CERTs) might be a good format for closer engagement, although they have limitations in terms of what they can do given that they lack enforcement powers. Europol and Interpol should also serve as platforms for cooperation.
- Improving information-sharing channels between private sector actors is also desirable. Some participants noted that when there are issues of suspected crime or fraud, the private sector does not always want to act, as it may adversely affect the company's image. Therefore, they often rely on personal or informal relationships to address such issues. More business-to-business (B2B) engagement on addressing cybersecurity issues could be implemented where legislation allows. Some work could be done through existing channels and frameworks, including Chambers of Commerce.

Cooperation on a public–private level is vital for both countries, despite the recent controversy regarding certain companies. This work should be intensified both on the national and international levels.

Information Security versus Cybersecurity: Different Approaches

When it comes to terms and conditions, Russia and the UK's conceptual approaches to 'cyber' appear significantly different. Each side's doctrines highlight some of the fundamental divergences in ways of thinking.

Russia's 2016 doctrine is devoted to ensuring the national security of the Russian Federation in the information space. This is defined as computer systems/software; information systems and websites within the information and telecommunications network of the internet; communication networks; information technology; and entities involved in generating and processing information, developing and using these technologies, and ensuring information security, as

well as mechanisms regulating relevant public relations.[20] The term 'cyber' is not used in Russian official documents.

One Russian expert stressed that the Information Security Doctrine, as well as other high-level strategic documents on information and national security are based on the concept of information space. Russia views information security as contributing to strategic stability, which is arguably broader than many Western definitions of the concept.

The expert also noted that like that of the US and the EU, the UK approach focuses mostly on protection of infrastructure and other assets in cyberspace. Because Moscow's concern over the destabilising impact of trans-border information flows is usually met with resistance from Western partners, the Russian Ministry of Foreign Affairs and other high-level decision-makers regard promotion of the cybersecurity narrative as an attempt to ignore major national interests and security concerns in the information space.

From the Russian perspective, threats are seen more in terms of the weaponisation or militarisation of information, whether they are from foreign states, terrorist and extremist groups or criminals. The doctrine is mainly about building up resilience to this by coordinating the 'information security forces', defined as government bodies, local authorities and organisations that address information security issues, and improving the broader information security system.

The UK's National Cyber Security Strategy 2016–2021 talks about information security, but in the sense of protecting data from malicious activity or breaches, not the weaponisation of information. It focuses more directly on cyberattacks as the main threat and the need to improve cybersecurity, namely the 'protection of information systems (hardware, software and associated infrastructure), data on them, and the services they provide from unauthorised access, harm or misuse'.[21] It also specifically categorises threat actors as cybercriminals; states and state-sponsored threats; terrorists; 'hactivists'; and script kiddies. Therefore, it shares the Russian view that threats are emanating from other governments, as well as criminals.

The UK Cyber Strategy also reflects some of the difficulties in agreeing on 'rules of the game' through examining approaches to defensive and deterrent measures, which is particularly relevant to the Russian debate. Both Russia and the UK emphasise defensive measures, but the line is more blurred between offensive, defensive and deterrent measures. For example, the strategy discusses using Active Cyber Defence measures, which means implementing security measures to 'strengthen a network or system to make it more robust against attack'. This is a proactive approach aimed at making UK systems a much harder target, and experts noted that at times the lines may be blurred between offensive and defensive approaches. British experts also commented on how certain Russian activities could be construed as a form of such active cyber defence.

[20] The Ministry of Foreign Affairs of the Russian Federation, 'Doctrine of Information Security of the Russian Federation', 5 December 2016.
[21] HM Government, 'National Cyber Security Strategy 2016–2021', 1 November 2016.

For example, Russia is developing legislation to ensure that the majority of Russian internet traffic is routed through the country by 2020.[22] One UK expert said this 'sounded like active cyber defence' to them.

Although one Russian expert saw a chance to achieve mutual understanding on these conceptual differences, generally the group was quite sceptical. However, the evolution of threats might allow some space for bilateral dialogue. For instance, the global IT industry is shifting its focus away from ensuring cybersecurity in terms of the traditional 'CIA' triad (Confidentiality, Integrity, Availability) to ensuring cyber resilience. The latter implies that there is currently no way to prevent all computer attacks and other security incidents, so information systems and infrastructures should be able to perform critical functions even when under attack or during the incident. The concept and notion of cyber resilience is stressed in the UK National Cyber Security Strategy 2016–2021. At the same time, similar concepts are reflected in the recent wave of regulatory activities in Russia aimed at ensuring the security of critical information infrastructure (CII) and best practices in the private sector. Still, state involvement in cyber activity will mean such discussions are challenging.

Some Russian experts claim that the state of information cyberspace is a major challenge to international security, and thus requires a collective assessment by the international community. It increasingly becomes a muddy pool, where all sorts of actors, including criminals and terrorists, can pursue their ends with impunity. Like any other area of international relations, global informational cyberspace requires coherent international legal regulation. Particularly what is needed is a universal set of legally binding norms that would provide detailed language for states' existing obligations, set procedures for establishing their violations, and help determine perpetrators. It is necessary to agree on procedures for the peaceful resolution of disputes, including the creation of a network of relevant national and multilateral mechanisms. Needless to say, this might require a long time to become feasible. According to some experts from Russia, if needed, amendments should be developed to existing international instruments, initially the prevention of international conflicts and dispute resolution. Logically, this will require setting up boundaries of states' sovereignty in this environment. Several participants believed that the grave US–Russia crisis resulting from accusations of Russia's 'interference in the political process in the US' should not be wasted, for it provides an additional incentive for such dialogue.

The Challenges of Defining 'Rules of the Game'

Given the differences in the conceptual approaches to 'cyber' issues of the UK and Russia, as well as the grey area concerning defensive versus offensive measures, there are unlikely to be any official bridges between the two countries. However, it is notable that this is not unique to the Russia–UK relationship. Even among allied Western countries, there is a lack of agreement on how to define

[22] Ministry of Telecom and Mass Communications of the Russian Federation, 'State program "Information society"' (Minkomsvyaz Rossii, Gosudarstvennaya Programma "Informatsionnoe obschestvo"), 21 August 2017.

the threat and the response. For example, a US Congressional Bill that proposed allowing companies to legally 'hack back', phrased as active cyberdefence, shows the spectrum of conceptual and legal thinking on this.[23] The US would also consider using nuclear weapons against a country or group that delivered a serious cyberattack against its critical infrastructure.[24]

Trying to determine norms, therefore is not necessarily linked to a downturn in Russia–West relations. However, it is due to the universal difficulty in drawing 'red lines' in a virtual world, particularly where hostile cyberactivity can take place just under any threshold of what is deemed to be force or malign activity. Moreover, certain activity perceived as hostile can be redefined as an effective defensive or deterrent measure depending on who uses it. To some hostile cyber-actors, defining 'red lines' or ring-fencing certain areas of critical infrastructure simply presents a set boundary, just under which activity can be conducted without triggering much of a response. Determining norms between governments in relation to cyber will continue to be challenging, fundamentally because, as one participant noted, they are simply 'too valuable' for states 'not to use them' in certain contexts.

An additional general difficulty comes when determining the source of any hostile activity or attack. Norms can be agreed on, but determining when one has been violated is challenging when attribution is, as one participant noted, 'notoriously hard'. It is easy to be wrong, as locations can be manipulated through IP addresses and Virtual Private Networks, and attacks could be conducted under false flags. This can undermine any legitimate attempts to justify accusations and counterattacks.

Even if norms could be defined, the mechanisms for enforcing them at an international level are unlikely to work in practice. The best-known initiatives on this include the work done by the UN Group of Government Experts (UN GGE) and the Tallinn Manual. The latter tries to highlight, for example, how international law and self-defence apply to cyber-operations, but there is often divergence in interpretation of these concepts between countries, often for political gain, as well as an absence of any real enforcement mechanism. Moreover, countries such as China and Russia are reticent to retrofit issues including cyberactivity into existing international law frameworks, toward which they often have their own grievances. Initiatives such as the Council of Europe's Budapest Convention[25] suggest legislative norms to combat hostile cyberactivity, but Russia has not signed up to this. It cites opposition to article 32, which allows permission of trans-border access to stored computer data during cybercrime investigations. Russia prefers instead to work within the UN to propose its own project.

A Russian expert noted that the UN draft convention 'On Cooperation in Countering Informational Crime', presented by Russia in Vienna in 2017, was another

[23] Congressman Tom Graves, 'Representative Tom Graves Proposes Cyber Self Defense Bill', press release, 3 March 2017.
[24] David E Sanger, 'Nations Seek the Elusive Cure for Cyberattacks', *New York Times*, 21 January 2018.
[25] Council of Europe, 'Convention on Cybercrime' Budapest, 23 November 2001.

attempt to bring the issue to a more global, UN, level.[26] It criminalises 14 online activities including unlawful interception and changing of data, disruption to the work of computer networks, creation of viruses and malware, cybertheft, violation of copyright laws, distribution of child pornography, and others. The expert also stresses that one of the important messages of the initiative is in the very approach to tackling these challenges. It stems from respect of national sovereignty and refraining from unlicensed trans-border access to stored data for investigation needs. So far, it does not seem to have overwhelming support in the international community, but is very consistent with Russia's general preference of tackling global problems through established multilateral channels and platforms. Meanwhile, in the absence of a universally recognised legal instrument, Mutual Legal Assistance Treaties (MLATs), alternative regional or bilateral agreements, as well as less formal channels, facilitate, to a degree, cooperation on cybercrime, assuming a favourable geopolitical context.

Certain progress could be made in a bilateral format as well. There have been some agreements at the bilateral level. For example, in April 2015, Russia signed an agreement with China to cooperate in the field of international information security.[27] At the September 2017 BRICS summit in China, Russia signed an agreement with South Africa[28] on information security. The US and UK cooperate on cybersecurity, particularly through intelligence sharing.[29] Bilateral agreements clearly seem easier to forge on issues related to cyber rather than at the multinational level, but they can also be vague in substance and more for diplomatic ceremony.

That is not to say that discussions on norms or rules are pointless, but simply that expectations should be managed as to what concrete decisions and agreements the discussion will lead to. Discussions can, however, provide useful means of communication to better understand the conceptual thinking and interests of states involved. In a bid to be realistic, discussions about norms should also not ignore the fact that cyberspace is another domain, which, like land and sea, will be leveraged for competitive advantage.

According to another Russian expert, many assume that because cyberspace is being militarised and cyber tools are becoming offensive, this should offer a seemingly logical and straightforward approach to defining red lines, critical infrastructure and objects of attack and defence, among other things. However, this approach fails primarily because of the nature of cyberspace (and information space). Actors operate in the virtual space of strategic – technically and lawfully deniable – ambiguity, which is unacceptable as a starting point for developing 'cyber arms control' treaties.

[26] *RT*, 'Russia Prepares new UN Anti-Cybercrime Convention – Report', 14 April 2017.
[27] The Russian Government, 'Signing a Russian-Chinese intergovernmental agreement on cooperation in ensuring international information security', 30 April 2015.
[28] The Ministry of Foreign Affairs of the Russian Federation, 'Press Release on Signing a Cooperation Agreement Between the Government of the Russian Federation and the Government of the Republic of South Africa on Maintaining International Information Security', 1622, press release, 4 September 2017.
[29] The White House, 'FACT SHEET: U.S.–United Kingdom Cybersecurity Cooperation', press release, 16 January 2015.

This expert added that while it seems that military operations in the cyber-domain are becoming a natural part of full-spectrum conflict, those operations are hard to separate from conventional warfare. Therefore, the problem transforms the limits of permissible cyber – and informational – intervention in peacetime, where some rules and norms can be developed.

Given the difficulties of inter-state cooperation on these issues, there is a need to encourage and amplify existing cooperation between technical communities.

Leveraging Private Sector and Technical Expertise

Despite political tension, there are clearly common security threats emanating from the criminal cyberworld. Although some policymakers may still be sceptical about Russia–UK cooperation on this, due to a low level of trust, the threat is clearly real and does not recognise borders. For example, the Cobalt criminal group hit banks in Russia, the UK, the Netherlands and Malaysia.[30] MoneyTaker targeted the Russian financial system, as well as US banks and a UK financial software provider.[31] Looking at evolving and future risks is also important, as terrorist groups are improving offensive cyber-capabilities.

Small steps could be taken at the government level. For example, establishing a UK–Russia cyber-hotline for reporting criminal activity could be a logical initiative, particularly due to the 2018 FIFA World Cup being held in Russia this summer. Once the line is established, clear rules of its operation should be introduced.

However, private sector and technical expertise provide good case studies of where constructive dialogue and practical cooperation have produced results in combating crime. The operation that led to the dismantling of the Avalanche criminal platform is an ideal example of how cooperation can and should work. This benefited from partnership between law enforcement agencies of multiple countries; multilateral law enforcement organisations, such as Europol; the private sector; and non-profit organisations, such as ICANN and Shadowserver. Not-for-profit organisations can be particularly useful in mediating between third parties, assisting countries that may not normally work together for political reasons.

Such operations are not without their challenges, however. An issue specific to the Avalanche operation was the lengthy legal processes required to enable collaboration, enabled through the MLATs. Although this slowed down the process, it did not prevent success. Streamlining information sharing where desirable and relevant would be beneficial. Long-term investment is also required for such operations. Indeed, the operation lasted more than four years. Law enforcement and the private sector should be prepared to invest such time and resources in this type of case.

Another issue is related to legal compatibility for extra-territorial cooperation.

[30] Group IB, 'Cobalt: Logical Attacks on ATMs: Report Outlining Activity of the Cobalt Hacker Group Attacking Banks in Europe and Asia'.
[31] Group IB, 'MoneyTaker: In Pursuit of the Invisible', 11 December 2017.

UK law enforcement was unable to fully work on Avalanche given the lack of domestic legislation governing this. Germany used criminal legislation for this, while the US used civil legislation for a temporary restraining order. CCTLD did not have the internal regulation to do this at the time but participated at its own risk. Since then, its board has approved such regulation, highlighting an example of a goodwill measure that paid off in a cooperative environment.

Further discussion about what platforms and what modalities of cooperation could work domestically and bilaterally would be useful. At the more inter-state level, it was suggested that CERTs might be a good format for closer engagement. However, there are limitations. CERTs are not always eligible to act, especially when it comes to law enforcement. Using formal law enforcement channels at the Russia–UK bilateral level can be difficult, given political tensions, but there are still ways to communicate at such levels either through other political channels or through third countries. Something more informal could help supplement this. Non-profit organisations with deep expertise proved useful in the Avalanche case, but some states may not consider them as legitimate as other actors.

At the private sector level, there is often greater flexibility in decision-making, which can make action more efficient compared with that which is reliant on public sector decisions. However, there is still a need to improve channels and motivation for sharing information between private sector stakeholders to ensure that risks are addressed. For example, some participants noted that when there are issues of suspected crime or fraud, the private sector does not always want to act, as it quickly becomes public and may affect a company's image. Therefore, they often rely on personal or informal relationships to address such issues. More business-to-business engagement on addressing cybersecurity issues could be implemented where legislation allows. However, this alone will not provide for prosecutions or deterrence, hence the need for a joined-up approach between the private and public sectors.

IT companies tend to face similar problems regardless of their location. For example, one representative from a Russian company noted the lack of collaboration on dealing with fraudulent accounts, as well as a lack of knowledge sharing. If someone has proof that a specific account is being used in a fraud scheme or any other kind of abuse, there is very little to do apart from reporting the abuse or contacting the support team and hoping for the best. For those professionally involved in dealing with fraud and cyber-abuse, there should be a framework to share information about malicious activities. That might help internet providers to act on fraudulent accounts for the sake of a safer internet.

Better public sector to private sector trust-building could also be helpful. Moreover, there is an added concern that enforcement against cybercrime is being outsourced to the private sector. As one UK expert put it, it was 'not the private sector's job to catch criminals, but their interest is to protect their client'. The public and private sector relationships in this space have also been mired in controversy.

Private Sector Risks

Although there could be more private-to-private and public-to-private sector co-operation, there are still obstacles to this in the UK–Russia and West–Russia relationship. Suspicions over political interference in private sector firms and software clearly hamper engagement. Moscow countered this in 2015 by prohibiting the purchase of foreign-produced software for its government's needs. Although part of Russia's policy of import substitution,[32] this was also due to perceived risks around foreign companies using their software to undermine Russian cybersecurity.

The most controversial case in the West is the accusation that firms such as Kaspersky have links with the Russian security services. This culminated in the US[33] and UK[34] publicly and explicitly pointing to risks concerning Kaspersky's anti-virus products in government departments, removing them from approved vendors lists in the case of the US. Stated concerns from the US and the UK mainly centred on the fact that it is a Russian product, highly intrusive by nature of its objective, and that there are suspected links between the company and Russian intelligence.

During the workshop, Kaspersky presented its defence, stating that it only transfers data that is relevant to fulfilling its contractual obligations; that there is a lack of evidence to back up accusations that there are ties between Kaspersky and any Russian officials; and that, given that Kaspersky is not a telecommunications company, it does not have a legal obligation to provide data to the Russian authorities as per recent legislation[35] (as suggested by the US). Kaspersky has filed a lawsuit, stating that allegations against the firm were 'arbitrary and capricious and not based on substantial evidence', and violated its right to due process.[36]

The company has now launched its Global Transparency Initiative, aimed at increasing information security policies and practices. Practically, the initial phase will include establishing Transparency Centres globally that will serve as a facility for trusted partners to access reviews on the company's code, software updates, and threat detection rules, along with other activities, as well as commencing an independent assessment of the company's secure development lifecycle processes, and its software and supply chain risk mitigation strategies.

The difference in approaches to assessing Kaspersky risks, however, was noted. The UK's National Cyber Security Centre (NCSC) engaged with Kaspersky during its risk analysis, which was appreciated. This was allegedly in contrast to

[32] Ministry of Telecom and Mass Communications of the Russian Federation, 'Russia's Policy of Software Import Substitution' (Prikaz Minkomsvyazi Rossii 'Ob utverzhdenii plana Importozameschenia programmnogo obespecheniya').
[33] Department of Homeland Security, 'DHS Statement on the Issuance of Binding Operational Directive 17-01', press release, 13 September 2017.
[34] National Cyber Security Centre, 'Letter to Permanent Secretaries Regarding the Issue of Supply Chain Risk in Cloud-Based Products', 1 December 2017.
[35] See Max Seddon, 'Russian Telecoms Groups Mount Fight against Anti-Terror Law', *Financial Times*, 11 July 2016.
[36] Thomas Fox-Brewster, 'Here's Kaspersky's Full Complaint Against The DHS Over Anti-Virus Ban', *Forbes*, 19 December 2017.

the US approach, which did not take Kaspersky's opinion into account. Part of the difficulty is that the justification for the perceived high risk of certain private sector activities cannot necessarily be publicly justified with hard evidence when governments may use sensitive information in this assessment or do not wish to reveal the knowledge and tools they use to determine such risk.

Still, this case also demonstrates that even if there are concerns, there is still an opportunity to engage with the relevant private sector actors to determine the risks. NCSC director Ciaran Martin noted 'we are in discussions with Kaspersky Lab … about whether we can develop a framework that we and others can independently verify'.[37] It often appears that assumptions are made about all Russian or Western companies operating in this sphere without attempts to understand how private sector actors work.

[37] National Cyber Security Centre, 'Letter to Permanent Secretaries Regarding the Issue of Supply Chain Risk in Cloud-Based Products', 1 December 2017.

About RIAC and RUSI

The Russian International Affairs Council (RIAC) is a non-profit international relations think-tank on a mission to provide policy recommendations for all of the Russian organizations involved in external affairs. RIAC engages experts, statesmen and entrepreneurs in public discussions with an end to increase the efficiency of Russian foreign policy. Along with research and analysis, the Russian Council is involved in educational activities to create a solid network of young global affairs and diplomacy experts. RIAC is a player on the second-track and public diplomacy arena, contributing the Russian view to international debate on pending issues of global development. Members of RIAC are the thought leaders of Russia's foreign affairs community – among them diplomats, businessmen, scholars, public leaders and journalists.

President of RIAC Igor Ivanov, Corresponding Member of the Russian Academy of Sciences, served as Minister of Foreign Affairs of the Russian Federation from 1998 to 2004 and Secretary of the Security Council from 2004 to 2007.

The Director General of RIAC is Andrey Kortunov. From 1995 to 1997, Dr. Kortunov was Deputy Director of the Institute for US and Canadian Studies.

The Royal United Services Institute (RUSI) is the world's oldest and the UK's leading defence and security think tank. Its mission is to inform, influence and enhance public debate on a safer and more stable world. RUSI is a research-led institute, producing independent, practical and innovative analysis to address today's complex challenges. Since its foundation in 1831, RUSI has relied on its members to support its activities. Together with revenue from research, publications and conferences, RUSI has sustained its political independence for 185 years.

About the Authors

Andrey Kortunov is the Director General of the Russian International Affairs Council (RIAC).

Malcolm Chalmers is Deputy Director-General of the Royal United Services Institute (RUSI).

Sarah Lain is an Associate Fellow at RUSI, where she focuses on Russian foreign policy. She previously worked in private sector consultancy, examining business risks in Russia and post-Soviet countries.

Maria Smekalova is the Coordinator of Cybersecurity Programmes at the Russian International Affairs Council (RIAC).

RUSSIAN INTERNATIONAL AFFAIRS COUNCIL (RIAC)
1, B. Yakimanka street, 119180, Moscow, Russia
Tel.: +7 (495) 225 6283
Fax: +7 (495) 225 6284
E–mail: welcome@russiancouncil.ru
www.russiancouncil.ru