EUROPEAN LEADERSHIP NETWORK

Building better security for wider Europe

Living in (Digital) Denial: Russia's Approach to Cyber Deterrence

EURO-ATLANTIC SECURITY REPORT

Joss Meakins

July 2018

About the Author

Joss Meakins works as a researcher at the ELN, focusing on Russia-West relations and cyber deterrence. His research interests include NATO-Russia arms control, cybersecurity and European defence. Joss studied languages at Cambridge and Russian security at Columbia University. He has previously interned at RUSI, researching the radicalisation of Central Asian migrants in Russia. Joss has been published in the International Journal of Intelligence and Counterintelligence, RUSI Defence Systems and the Washington Post. He speaks fluent Russian.

The European Leadership Network (ELN) works to advance the idea of a cooperative and cohesive Europe and to develop collaborative European capacity to address the pressing foreign, defence and security policy challenges of our time. It does this through its active network of former and emerging European political, military, and diplomatic leaders, through its high-quality research, publications and events, and through its institutional partnerships across Europe, North America, Latin America and the Asia-Pacific region.

Living in (Digital) Denial: Russia's Approach to Cyber Deterrence

In an era of ever more alarming cyberattacks, Western policymakers are increasingly looking to the concept of 'cyber deterrence' as a force for stability. Understood as the ability to dissuade enemy attacks through the credible threat of retaliation, deterrence looms large in discussions of Russian cyberattacks. However, for such a deterrence relationship to work, it must at least be tacitly accepted by the other side. Yet the Russian strategic community currently appears highly critical of cyber deterrence, with many officials and experts deriding the concept as unworkable.

This report examines key Russian theoretical objections, alongside Russia's practical, albeit partial, implementation of the concept. Indeed, in spite of sustained criticism, the Russian position on cyber deterrence has in some ways come to mirror that of the West.

Even so, unless Russia fully embraces the concept, instability and the risk of unintended escalation will remain. Thus, Western policymakers need to convince and incentivise Russia to accept cyber deterrence as a stabilising framework. This requires Western countries to:

- Improve their cyber deterrence posture by drawing select and credible red lines, such as a declaration that attacks on critical national infrastructure will incur a response.

- Build allied capacity and cyber defences to better withstand and mitigate attacks, thereby increasing the cost of attacks and deterring Russia through denial.

- Engage Russia in a multiyear, governmental dialogue on cyber issues to argue the case for cyber deterrence and address Russian objections.

The long-term goal of such efforts should be to eventually reach a politically binding agreement with Russia on acceptable behaviour in cyberspace. This would cover:

1. Non-interference in political processes.
2. Refraining from attacks on critical national infrastructure.
3. Refraining from attacks on the 'public core' of the internet.
4. Agreeing common standards for attribution.
5. Agreeing that attacks on nuclear command and control are impermissible.

Although these aims are ambitious, they are the best solution for creating lasting West-Russia stability in cyberspace.

'Therefore, if you wish, your little pug in Europe may bark at the Russian cyber-elephant.'[1]

- Andrey Krutskikh, (Special Representative of the Russian President for Information Security)

Introduction

To address increasing instability in cyber-space, British and American policymakers are increasingly looking to the idea of 'deterrence', the ability to dissuade enemy attacks through the credible threat of retaliation. The UK's National Cyber Security Strategy 2016-2021[2] places significant emphasis on deterrence and, in spite of certain theoretical complexities outlined below, cyber deterrence may still offer a potential framework for instituting greater predictability and stability in cyberspace. However, it is far from clear that the Russian strategic community will agree with this concept, let alone accept it. Indeed, although there has been much research on Russia's recent cyber conduct,[3] there has been very little focus on the Russian approach to cyber deterrence. By examining the articles, speeches and interviews of Russian officials and policymakers, in this paper, I will analyse the Russian viewpoint and evaluate the implications for Western[4] governments.

Many Russian policymakers, academics and strategists appear highly critical of cyber deterrence and believe it to be an unworkable construct. These views are rooted partly in a distinctly Russian conception of cyber as one indivisible element within a broader deterrence strategy, and partly in Russian scepticism about applying nuclear deterrence theory to cyberspace. However, in spite of these objections, Russian officials seem to publicly espouse a cyber deterrence policy in all but name, largely in reaction to a perceived (cyber) arms build-up by the West. According to the Russian narrative, it is the West's destabilising pursuit of offensive cyber capability which is forcing Russia to respond and reciprocate.

This contradiction between Russian theory and practice seems to have three causes. Firstly, many Russian thinkers appear to have genuine reservations about the feasibility of deterrence in cyberspace. These issues are explored below and centre on the difficulties of attribution and possibility of dangerous miscalculation and are shared at least in part by some in the West.[5] Secondly, Russian criticism of cyber deterrence is also, to some extent, a self-serving attempt to divert attention from Russia's aggressive cyber operations abroad and hinder international pressure for greater regulation. Finally, disagreements within Russia's defence and strategic community may also help to explain the dissonance. It is notable that many academics and Russian diplomats have long lobbied for international cyber agreements. I suggest that this lobby, which sees greater regulation as being in Russia's long-term interest, has been side-lined by more 'hawkish' elements, particularly within the

1 Adapted from a Russian fable 'The Elephant and the Pug', quoted in 'Спецпредставитель Путина рассказал о желании выпить и обозвал Европу "моськой", а РФ назвал "киберслоном'', UNIAN, 17 April 2018

2 'UK National Cyber Security Strategy 2016 to 2021', 1 November 2016, p.46.

3 Michael Connell and Sarah Vogler, 'Russia's Approach to Cyber Warfare', *Centre for Naval Analyses*, March 2017

4 Some would question the idea of a unified Western position on cyber deterrence. Thus, in this report, I will use 'Western' primarily as shorthand for British and American policy as these are the two Western powers most invested in cyber deterrence and with the most advanced cyber offensive capabilities. Nevertheless, NATO's extension of Article 5 to cyberattacks and recognition of cyberspace as a domain of operations arguably mark the first steps towards a unified Western cyber deterrence posture.

5 Michael P. Fischekeller and Richard J. Harknett, 'Deterrence is Not a Credible Strategy for Cyberspace.' *Orbis*. Vol. 61, Issue 3, 2017, pp.381-393

intelligence services, who want all options to be available and see deterrence as a check on Russian power projection.

> ***"Russian criticism of cyber deterrence is, to some extent, self-serving."***

The resultant implications for policymakers will be examined at the end of this paper but the key conclusion is the need to convince Russia of the credibility and value of cyber deterrence. While Russia's commitment to the concept remains incoherent and incomplete, the risk of serious, unintended escalation will remain. The West can shift the Russian position in two ways. Firstly, by improving its own cyber deterrent posture, establishing credible red lines and making clear to Russia that significant cyberattacks will incur significant costs. Similarly, improving cyber defence across government and wider society systems is vital to raise the cost of attacks, thereby deterring Russia by denial. These measures will raise the credibility of the Western cyber deterrence model, incentivising Russia to follow suit and embrace cyber deterrence as a framework for stabilisation. Secondly, however, Western policymakers must continue to engage their Russian counterparts in bilateral and multilateral discussions to argue the case for cyber deterrence. Although such a process could take years, the eventual goal should be to create a Russia-West agreement on cyber norms as the only long-term solution to current instability.

Applying Deterrence Theory to Cyberspace

Deterrence can be defined as 'dissuading someone from doing something by making them believe that the costs to them will exceed the expected benefit.'[6] The Cold War marked the heyday of deterrence theory, particularly with regard to nuclear weapons. Yet several experts and policymakers see an application for the concept in cyberspace today.[7][8] Traditionally, deterrence is accomplished through the threat of retaliation (deterrence by punishment), or by denying an enemy the ability to inflict real damage (deterrence by denial), or some combination of the two.[9] Protecting all networks all the time is difficult, yet even modest increases in security across national networks can dramatically improve cyber defence and reduce the likelihood of successful attacks.[10] Thus, an effective cyber strategy will leverage both forms of deterrence to dissuade attacks.

Applying this theoretical framework to cyber operations in today's world is complicated by several aspects unique to cyberspace. Cyber weapons differ from nuclear ones and this impacts their deterrent effect. Firstly, cyber weapons can be used in ways that do not inflict physical damage or casualties. Secondly, cyberattacks are instantaneous with little to no warning. Thirdly, attribution of an attack is usually very complicated and time consuming, although not impossible.[11] Fourthly, a state's cyber capabilities will change continuously, as zero-day[12] stockpiles change and software is updated. Fifthly, most cyber weapons must remain secret to be effective. If the US discovers a software vulnerability in Russian military systems, they cannot explicitly threaten to make use of it without alerting the Russians to the flaw. This potentially reduces the credibility of a national cyber deterrent as each nation's exact capabilities remain unknown. Finally, conducting cyber espionage (CNE) requires almost the same degree of network penetration as conducting a cyberattack (CNA). This knowledge may encourage worst-case assumptions about an adversary's intent and prove destabilising for signalling in cyberspace.

> ***"Several experts and policymakers see an application for cyber deterrence today."***

As noted above, these differences have led some to argue that deterrence in cyberspace is not possible. However, differences between cyberspace and the nuclear realm may also help to enable cyber deterrence. The devastating power of nuclear weapons can make a single deterrence failure catastrophic. The deliberate use of a nuclear weapon by one state against another would change the world irrevocably and quite possibly spark a wider conflict. By contrast, cyber deterrence will only ever be a best-effort attempt. Much like deterrence in law enforcement, the aim is to deter major and widespread infractions, not every attack all the time.[13] Moreover, unlike a retaliatory nuclear strike, the response to a cyberattack need not necessarily be immediate or in kind to be effective. Other tools like sanctions, diplomatic pressure or

6 Joseph S. Nye Jr., 'Deterrence and Dissuasion in Cyberspace.' *International Security*. Vol. 41, No. 3 (Winter 2016/17), p.45

7 'Department of Defense - Defense Science Board: Task Force on Cyber Deterrence', February 2017

8 Christopher Paul and Rand Waltzman, 'How the Pentagon Should Deter Cyber Attacks', *RAND*, 10 January 2018

9 Michael Rühle, 'Deterrence: what it can (and cannot) do', *NATO Review Online*

10 David T. Fahrenkrug, 'Countering the Offensive Advantage in Cyberspace: An Integrated Defensive Strategy', *NATO CCD COE*, 2012

11 Thomas Frear, 'Inherent Instability: Cyber and Space as Deterrence Spoilers', *European Leadership Network*, 14 March 2018

12 A zero-day is a previously unknown software vulnerability which can be used to exploit a device, system or application.

13 Derek B. Johnson, 'Cyber deterrence is about more than punching back', *FCW*, 10 May 2018

limited military strikes may potentially offer a compelling response to cyberattacks. Thus, although cyber deterrence may differ from nuclear deterrence, it can help to prevent the most destructive cyberattacks, 'above the threshold of death and destruction.'[14]

Nevertheless, as Martin Libicki notes, the issues of attribution and thresholds continue to complicate cyber deterrence.[15] The ability to identify one's attacker is essential to deterring them. However, doing so is complicated by the widespread availability and use of human and technical proxies. Moreover, faulty attribution could lead to an unprovoked attack or even war. Similarly, identifying an attacker may involve the use of covert sources and methods which cannot be divulged, thus complicating efforts to convince a public and international community demanding 'proof'. This would be a particular concern for countries seeking to trigger NATO's Article 5 in response to a cyberattack. Finally, a state wishing to deter cyberattacks must define what constitutes an attack and what the response would be. Setting the threshold too low means having to respond to all attacks or risk losing credibility. Setting it too high risks giving adversaries a precise idea of what they can get away with, allowing them to wreak havoc just short of the line. This dilemma also arises when deterring 'hybrid operations' which stop short of any overt red lines yet can cause great harm nonetheless.

Even so, cyber deterrence remains a valuable, if imperfect, framework for preventing the most devastating state-on-state cyberattacks and forging norms for international behaviour in cyberspace.[16] The essential secrecy surrounding cyber weapons, alongside their intrinsic utility and the current political climate make the prospects for cyber arms control doubtful. As Peter Singer notes, pursuing an integrated cyber deterrence strategy is one of the few ways to bring order and greater predictability to cyberspace.[17] For Western countries, stating publicly that attacks on critical national infrastructure (CNI), for example, will be met with proportionate but credible retaliation is a key step in establishing impermissible cyber conduct.

> ***"The issues of attribution and thresholds continue to complicate cyber deterrence."***

Furthermore, although it is often difficult to identify one's attacker in cyberspace, the US and British governments have publicly attributed several recent cyber-attacks to nation-states. Examples include: Sony, NotPetya, WannaCry, the DNC hack and the targeting of US energy networks.[18] To continue the crime fighting comparison, the combination of motivation and technical/human indicators in these cases allowed for attribution 'beyond reasonable doubt'[19] and retaliatory measures to discourage such behaviour in the future. Although some deemed the punishment insufficient in these cases, attribution is the first step to effective deterrence. Like nuclear deterrence theory at the start of the Cold War, cyber deterrence theory and practice is evolving and as it matures, it can be made more refined and useful.

14 Adam Segal, 'Not The Cyber Deterrence the United States Wants', Council on Foreign Relations Blog, 11 June 2018

15 Martin C. Libicki, 'It Takes More than Offensive Capability to Have an Effective Cyberdeterrence Posture', *RAND*, Congressional Testimony, 1 March 2017

16 Libicki, *op. cit.*

17 Peter W. Singer, 'Cyber-Deterrence And the Goal of Resilience: 30 New Actions That Congress Can Take to Improve U.S. Cybersecurity', *Testimony to the House Armed Services Committee*, 1 March 2017

18 'Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors', *US-CERT Joint Technical Alert (DHS & FBI)*, 15 March 2018

19 Justin Harvey, 'The shadowy—and vital—role attribution plays in cybersecurity', *Accenture Security Blog*, 4 May 2017

Deconstructing cyber deterrence in Russian strategic thought

Defining the Russian approach to cyber deterrence is complicated by several factors. Firstly, in Russian strategic literature, the term deterrence is most commonly applied to the idea of 'strategic deterrence.' As defined by the 2014 Defence Doctrine, this concept encompasses both nuclear and conventional force.[20] Moreover, according to the 2015 National Security Strategy, strategic deterrence is designed to prevent armed conflict and is accomplished via 'Interrelated political, military, military-technical, diplomatic, economic, informational, and other measures.'[21] Thus, the Russian deterrence construct is more holistic than NATO definitions, seeking to produce a combined deterrent effect through a range of military and non-military means.[22] Secondly, the Russian understanding of 'strategic deterrence' goes beyond Western deterrence, incorporating elements of coercion, compellence and containment 'to deter or dominate a conflict' rather than prevent any military action at all.[23] To Western eyes, this posture can seem more aggressive than defensive and arguably creates deterrence instability within the NATO-Russia relationship.[24]

> ***"The Russian deterrence construct is more holistic than NATO definitions."***

Thirdly, in contrast to Western military thought, in Russia deterrence is not conceptualised through separate 'conventional', 'nuclear', or 'cyber' domains. Instead, the Russians see cyber operations as a subset of 'Information Warfare', which itself makes up a key component of strategic deterrence. Information Warfare (IW) can be defined as 'carrying out mass psychological campaigns against the population of a State in order to destabilize society and the government; as well as forcing a State to make decisions in the interests of their opponents.'[25] It is a broad concept drawing on Soviet traditions of reflexive control, disinformation, maskirovka and provokatsiya[26] and covering Electronic Warfare, PSYOPS, Strategic Communications and Information Operations, as well as cyber.[27] As Sergey Ivanov (then Defence Minister) put it in 2007, 'It (IW) is a weapon that allows us to carry out would-be military actions in practically any theatre of war and most importantly, without using military power.'[28] In his famous 2013 article, Valeriy Gerasimov, Chief of the General Staff of the Armed Forces, wrote that 'information and psychological warfare will largely lay the groundwork for victory.'[29] Therefore, in Russian thinking, cyber operations can help to ensure strategic deterrence but only as a subset of IW, not as a domain in its own right. This contrasts with Western thinking, as shown by NATO's recognition of cyberspace as a domain of operations at the 2016 Summit, alongside air, sea and land.[30]

20 '2014 Military Doctrine of the Russian Federation', 26 December 2014, Point 32.b)

21 '2015 National Security Strategy of the Russian Federation', 31 December 2015, Point 36

22 Kristin Ven Bruusgaard, 'Russian Strategic Deterrence', *Survival*, 58:4, 2016, pp.7-26

23 Ven Bruusgaard, *op. cit.* p.7

24 Thomas Frear, Lukasz Kulesa and Denitsa Raynova, 'Russia and NATO: How to overcome deterrence instability?', *The European Leadership Network*, 27 April 2018

25 'Convention on International Information Security', 22 September 2011

26 John R. Schindler, 'The 9 Russian Words That Explain KremlinGate', *The Observer*, 28 March 2017

27 Stephen Blank, 'Cyber War and Information War à la Russe' in *Understanding Cyber Conflict: Fourteen Analogies* (Georgetown University Press: 2017), p.81 http://carnegieendowment.org/files/GUP_Perkovich_Levite_UnderstandingCyberConflict_Ch5.pdf

28 Blank, *op. cit.* p.84

29 Mark Galeotti, 'The 'Gerasimov Doctrine' and Russian Non-Linear War', *In Moscow's Shadows*, 6 July 2014

30 'Cyber Defence', *NATO website*, last updated 28 May 2018

Russian objections to cyber deterrence

Partly due to the Russian perception of cyber operations as a subset of IW and strategic deterrence more broadly, discussion of cyber deterrence in Russian sources is limited and largely focuses on criticism of the Western concept. Indeed, consensus opinion within the Russian strategic community holds that deterrence in cyberspace is not possible and that entertaining the idea would be dangerous and destabilising. In fact, five key objections can be identified in the Russian discourse and these will be explored in detail below. These criticisms do not appear to be just a smokescreen for Russian cyber aggression or repetition of some 'party line.' Rather, they surface repeatedly among different speakers in different contexts and seem to mostly reflect sincere concerns and objections.

1. The impossibility of accurate attribution

Foremost amongst these criticisms is the belief that accurately attributing attacks in cyberspace is impossible and this makes cyber deterrence untenable. This is a widely held Russian view, espoused by Gerasimov,[31] Andrey Krutskikh (the President's Special Representative for Information Security), Igor Ivanov (former Foreign Minister),[32] various Russian Defence Ministry officials[33] and prominent academics, including Valeriy Yashchenko, Deputy Director of Moscow State University's Information Security Institute.[34] Colonel Konstantin Peschanenko, a Representative of the Russian General Staff, expressed the same view at a recent conference, stating that accurate attribution is currently impossible, partly because there are no agreed international methodologies or criteria.[35] Similarly, Sergey Komov, Lead Researcher at the Military Academy of the Russian General Staff argues that without agreed methods for the collection of technical attribution indicators, it will not be possible to establish international standards or agreement on the topic.[36]

2. Cyberattacks as a false pretext for war

Such strongly held views on the unreliability of current attribution are also the key to another prominent Russian concern, namely that the Western adoption of cyber deterrence will greatly increase the risk of 'provocation', whereby a third party might deliberately trigger a cyber-war between two states. Here Komov agrees with Peschanenko that attempts at attribution without an international agreement on technical standards will lead to 'unfounded and mistaken accusations and, as a result, conflict escalation and a general reduction in the level of strategic stability.'[37] Krutskikh's assessment is blunter, 'The danger with cyber technology, and we have discussed this with the Americans in detail, is that someone might want to make us clash.'[38] He goes on to moot the idea of an ISIS hacker posing as the Russian government to carry out an attack

31 'Герасимов рассказал о военных последствиях кибератак', *RIA Novosti*, 26 April 2017

32 Igor Ivanov, '«Мутная вода» киберпространства', *Russian International Affairs Council,* 29 January 2018

33 Elena Chernenko and Ivan Safronov, 'К кибероружию примеряют ядерную модель', *Kommersant*, 23 March 2015

34 'Россия потратит $200-250 млн на разработку наступательного кибероружия', Habr, 9 February 2016

35 'Киберстабильность: подходы, перспективы, вызовы', *International Affairs,* Video playback from recent conference on cybersecurity, 42.25 to 42.37 seconds

36 'Россия и глобальные вызовы в области информационной безопасности', *International Affairs,* Special Edition*,* 15 April 2017, p.106

37 'Киберстабильность: подходы, перспективы, вызовы', *op. cit.* 43.34 to 43.46 seconds

38 Elena Chernenko, 'Россия сделает все, чтобы не проиграть киберсоревнование' *Kommersant*, 28 April 2016

against the US and sparking a war between the two powers. This concern is echoed by Major-General Igor Dylevskiy, Deputy Head of the Main Operations Directorate of the Russian General Staff.[39] Moreover, in 2017, Oleg Syromolotov, Deputy Head of the Russian Foreign Ministry warned that 'Cyber provocation can be used to lead states into confrontation and even wars.'[40]

> ***"If cyber weapons are the new WMDs, fabricated cyber aggression could provide a pretext for military action."***

Indeed, judging by speeches from representatives of Russia's military and security services at the conference 'InfoForum 2018', the perceived problems of faulty attribution and violent escalation are the primary Russian objections to cyber deterrence.[41] Some Russian thinkers go further, arguing that the cyber deterrence model could be used as a pretext for aggression or even a manufactured casus belli. As well as criticising attribution, Dylevskiy raises the issue of false flag attacks, arguing that cyber deterrence would allow a state to deceitfully claim to have suffered a cyberattack and use this as a false pretext for military strikes.[42] Although he does not make explicit mention of it, the spectre of Iraq looms large in Dylevskiy's analysis. If cyber weapons are the new WMDs, fabricated cyber aggression could provide a pretext for military action. Vladislav Sherstyuk, former director of FAPSI and current Director of Moscow State University's Information Security Institute raised similar concerns in 2017, 'When the problem of attribution is not solved, a perpetrator may simply be 'appointed' for political reasons, with not just sanctions but military measures brought against them.'[43] This concern is also frequently voiced in academic circles, with Nataliya Romashkina of the Primakov National Research Institute arguing that faulty attribution could lead to accusations based on 'assumptions to meet political goals.'

3. The risk to nuclear stability

The third key Russian objection to deterrence centres on the possibility of misattribution and miscalculation in cyberspace negatively impacting nuclear stability. According to Russian experts, this was demonstrated by the release of the 2018 US Nuclear Posture Review which allows for a nuclear response to 'significant, non-nuclear strategic attacks' (understood to include cyberattacks).[44] In official and academic circles the Russian reaction was vituperative. The Foreign Ministry released a press statement criticising the policy as destabilising.'[45] Konstantin Kosachev, Chairman of the Federation Council's Foreign Affairs Committee, said that linking a nuclear response to cyberattacks damages rather than increases deterrence and gives America carte blanche to engage in nuclear bullying.[46] For his part, Krutskikh made clear that the logic of nuclear deterrence cannot and should not be applied to cyberspace, declaring dramatically that 'Proponents of implementing deterrence

39 'IV Московская Конференция по Международной Безопасности', *Russian Ministry of Defence*, 26-27 April 2017, p.93

40 Elena Chernenko, 'К кибербезопасности подошли с трех сторон', *Kommersant*, 15 December 2017

41 Nataliya Romashkina 'Собрать киберпазл', *Russian International Affairs Council*, 22 February 2018

42 'IV Московская Конференция по Международной Безопасности', *op. cit.* p.95

43 Chernenko, 'К кибербезопасности подошли с трех сторон', *op. cit.*

44 Jeffrey Lewis, '"WannaCry" about Trump's Nuclear Posture Review? The global implications of deterring cyber attacks with nuclear weapons', *The Nuclear Threat Initiative*, 18 June 2018

45 'Комментарий Департамента информации и печати МИД России в связи с публикацией новой ядерной доктрины США', Russian Foreign Ministry, 3 February 2018

46 Konstantin Kosachev, 'Америка разрешает себе «ответить» ядерным оружием', *Echo of Moscow*, 4 February 2018

theory in cyberspace should understand that you can't have a competition on a minefield.'[47]

4. The unsuitability of deterrence to cyberspace

Indeed, the idea that the theory of nuclear deterrence is not applicable to cyberspace is a mainstay of Russian analysis and provides the fourth strand of criticism. Two primary arguments are cited by Russian analysts as evidence. Firstly, the inherently offense-oriented nature of cyber weapons, alongside their widespread use and availability make deterrence impractical. As Valeriy Yashchenko of Moscow State University argues, 'Offensive cyber technologies are now so widespread that it's not clear who would be deterring whom.'[48] Thus, Western attempts to institute a cyber deterrence framework are perceived as likely to have a destabilising, rather than deterrent effect.[49] Krutskikh extends the comparison, stating that cyber deterrence won't work because, 'Nuclear weapons are weapons of deterrence, cyber weapons are used every day and are used offensively.'[50] Secondly, some Russian strategists argue that cyber deterrence is hopeless because, unlike with nuclear weapons, there is no way for either side to check the other's capabilities or systems. This view is well expressed by Major-General Dylevskiy who contends that without verification, one side cannot trust the other and strategic stability cannot exist.[51]

5. The risk of an arms race

Finally, in Russian strategic literature, there is a widespread belief that the Western adoption of cyber deterrence will trigger a dangerous cyber 'arms race', threatening strategic stability. Dylevskiy is a key proponent of this argument[52] but it is clear that many others in the Military and Ministry of Defence share his viewpoint, with one source accusing the US of 'causing an arms race in this sphere.'[53] Similarly, Vadim Zapivakhin, a representative of the Russian General Staff, recently stated that the US position on cyber deterrence was causing 'an information arms race' which would damage strategic stability.[54] Peschanenko, another officer of the General Staff, was equally blunt in his assessment of the Western cyber deterrence concept as arbitrary and dangerous, stating that 'The path chosen by the West…..poses a direct threat and danger…..to the Russian Federation.'[55] This evident alarm in senior military circles, is perhaps a reflection of the Russian strategic perception of cyber weapons as finite and offense-oriented, with the advantage going to whichever side strikes first. Consequently, Russian military theorists tend to see cyber weapons as inherently destabilising and prone to cause unpredictable, possibly uncontrollable, escalation.[56]

47 'Нам не надо бороться за репутацию. Мундир наш и так чист', *Kommersant*, 23 April 2018

48 Chernenko and Safronov, *op. cit.*

49 Chernenko and Safronov, *op. cit.*

50 Anastasiya Tolstukhina, 'Мы не должны играть в безумства на взрывоопасном информационном поле', *International Affairs*, 29 April 2017

51 Igor Dylevskiy, 'Правила поведения в информационном пространстве — альтернатива гонке информационных вооружений', *Digital.Report*, 3 May 2016

52 Dylevskiy, *op. cit.*

53 Chernenko and Safronov, *op. cit.*

54 Tolstukhina, *op. cit*.

55 'Киберстабильность: подходы, перспективы, вызовы', *op. cit.* 44.55 to 45.08 seconds

56 'Toward U.S.-Russia Bilateral Cooperation in the Sphere of Cybersecurity', Working Group Paper 7, May 2016, p. 12

Russian cyber deterrence in practice

Nevertheless, in spite of vehement Russian objections to cyber deterrence, it should be assumed that within the Russian government, there have been discussions about how to dissuade and deter adversaries from conducting cyberattacks against Russia. However, official doctrine sheds no light on what these plans might be. Russia's 2016 Information Security Doctrine does not mention offensive cyber, fails to spell out how Russia would respond to an attack and seems almost totally focused on defence.[57] The same is true of the 2011 'Conceptual views on the activities of the Armed Forces of the Russian Federation in the information space.' This is demonstrated in Article 3.2, Point 3, 'In the event of a conflict in the information space escalating to crisis phase, (Russia) will exercise its right to individual or collective self-defence.'[58] This statement appears to be an assertion of fact rather than an attempt at deterrence signalling.

An analysis of public pronouncements shows several Russian officials espousing a cyber deterrence posture in all but name. Although such remarks fall short of official policy, loud warnings that Russia will retaliate if attacked are designed to deter aggression. As Krutskikh states, Russia 'will not forgive a single cyberattack'[59] and will 'never turn the other cheek.'[60] This message was communicated repeatedly in the aftermath of the Skripal case, when rumours circulated that Britain was considering retaliatory cyberattacks against Russia. In response, Krutskikh raged, 'Do the English think that Russia, having been hit, will just shrug it off? Do they really think they can mess about with Russia in cyberspace and that will go unanswered?'[61] Indeed, according to Andrey Kortunov, Director General of RIAC, had the UK conducted cyberattacks against Russia, Russia would have responded in kind.[62] In fact, some of Krutskikh's remarks echo the Western approach to cyber deterrence exactly. In 2017, he declared, 'We will not attack….But we will not let anyone attack us, we will defend both our citizens and our businesses.'[63] These statements seem aimed at deterring adversaries, thereby preventing attacks. Finally, while mulling the difficulties of proportionate cyber retaliation, Major-General Dylevskiy of the General Staff is unequivocal in his assessment that attacks on Russian energy infrastructure would be deemed 'an act of aggression.'[64]

> ***"Several Russian officials espouse a cyber deterrence posture in all but name."***

Moreover, according to Oleg Demidov, a cyber expert, the Russian Ministry of Defence has made clear on numerous occasions that cyberattacks against Russia will be answered but not necessarily in kind. In fact, Demidov states that 'the response to the use of force against Russia in the information space' would be of Russia's choosing.[65] This

57 '2016 Information Security Doctrine of the Russian Federation', 5 December 2016, Point 2.g

58 'Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве', 2011

59 'Спецпредставитель Путина рассказал о желании выпить и обозвал Европу "моськой", а РФ назвал "киберслоном', *UNIAN*, 17 April 2018

60 'Говорят участники международной конференции «Актуальные вопросы информационной и кибербезопасности»', *International Affairs*, 22 December 2016

61 'Крутских: попытки Великобритании навредить РФ в киберпространстве не останутся без ответа', *TASS*, 5 April 2018

62 Andrey Kortunov, 'Что может предпринять Великобритания и каким может быть ответ России?', *Russian International Affairs Council*, 14 March 2018

63 Aleksandr Kolesnichenko, 'Андрей Крутских: с кибербезопасностью все так же, как с ядерным оружием', *Argumenty i Fakty*, 25 May 2017

64 'IV Московская Конференция по Международной Безопасности', *op. cit*. pp.94-95

65 'Ракета в ответ на кибератаку?', *International Affairs*, 30 January 2017

is a clear articulation of Russian 'strategic deterrence', using all means available to deter to an attack. The closest Western concept is labelled 'cross-domain deterrence' and will be addressed more below.[66] Furthermore, atypically for a Russian scholar, Demidov argues that some sort of de facto cyber deterrence already exists between Russia and the US. Both parties can already hold each other at risk to some degree and this knowledge has at least some deterrent effect, as shown by the lack of outright and unrestricted cyber warfare between the two to date.[67]

> ***"Cyberattacks against Russia will be answered but not necessarily in kind."***

More importantly, in 2016 SC Magazine reported that Russia would spend $200-250 million on offensive cyber capabilities.[68] A spokesperson for the Federal Security Service (FSB) said that the announcement was intended to signal the creation of a cyber-deterrent directed at America. This individual stated that although creating a cyber deterrent is complex, Russia had been forced to do so by America's build-up of cyber weapons. This announcement seems to be a tacit admission that the West's adoption of cyber deterrence is gradually forcing a reluctant Russia to develop a similar deterrence posture in cyberspace. Indeed, in some ways, Russia's contradictory approach to cyber echoes the Soviet position on nuclear deterrence. As one Russian expert notes, 'nuclear deterrence itself was strongly criticised, but in practice the military-political leadership of the country followed precisely this principle.'[69]

Finally, in spite of furious Russian objections to the latest US NPR, there is reason to believe that Russian doctrine also allows for nuclear retaliation in the event of a devastating cyberattack. In accordance with Article 27 of Russia's 2014 Military Doctrine, nuclear weapons are only to be used when Russia is being attacked with nuclear weapons 'or other WMDs' or when 'the very existence of the state is threatened' by the use of conventional weapons.[70] In 2017, Krutskikh stated that cyber weapons were 'in terms of damage, completely comparable with the use of conventional weapons and, I think, in some cases, they can now be compared to WMDs.'[71] This echoes the opinion of Irina Yarovaya, a Deputy Chairwoman of the Duma, who said in 2016 that 'information weapons today are weapons of mass destruction.'[72] Given these comments and the devastating nature of a concerted cyber campaign against a country's CNI, it seems possible that a sufficiently damaging cyberattack could meet the 2014 Military Doctrine's threshold for nuclear retaliation.

66 King Mallory, 'New Challenges in Cross-Domain Deterrence', *RAND*, 2018

67 'Ракета в ответ на кибератаку?', *op. cit*.

68 Eugene Gerden 'Russia to spend $250m strengthening cyber-offensive capabilities', SC Magazine, 4 February 2016

69 Dave Johnson, 'Russia's Conventional Precision Strike Capabilities, Regional Crises, and Nuclear Thresholds', Livermore Papers on Global Security No. 3, February 2018, p.42

70 'Путин назвал две причины для применения ядерного оружия', *RBK*, 2 March 2018

71 'Крутских сравнил кибератаки с оружием массового поражения', *RIA Novosti*, 29 November 2017

72 'Россия и глобальные вызовы в области информационной безопасности', op. cit. p.97

Conclusions and recommendations

The Russian approach to cyber deterrence is marked by two paradoxes. Firstly, although there is broad consensus in Moscow that cyber deterrence is unworkable, Russian officials seem to espouse a cyber deterrence policy in all but name, relying on the threat of retaliation to deter major attacks. Secondly, while the Russian government conducts myriad aggressive cyber operations abroad, Russian officials and policymakers repeatedly warn about the destabilising nature of cyber weapons and the danger of a cyber arms race. The reasons for this discrepancy between thought and deed appear to be fourfold. Firstly, as outlined above, there does seem to be genuine Russian scepticism about the applicability of deterrence to cyberspace. As a Foreign Ministry official noted, there remains a lack of clarity within the Russian government about what a proportionate and appropriate response to cyberattack would be.[73] Secondly, however, although Russian concerns may be genuine, they are also self-serving. Broadly, the Russian position relies on a number of convenient arguments: cyberspace is dangerous and can't be regulated, Western attempts to do so are irresponsible and America's offensive capabilities are both destabilising and a threat to Russia. All of these arguments neatly draw attention away from Russia's unceasingly aggressive cyber campaigns against the West, as well as providing an excuse for Russian opposition to greater regulation.

Thirdly, as noted above, Russia's integrated approach to deterrence partly explains their objection to viewing cyber deterrence in isolation. Strategic deterrence encompasses multiple spheres, envisaging military, informational or other responses to a cyber threat. Yet even within this broader framework, there is significant Russian scepticism that cyber-attacks can be meaningfully deterred. As one scholar points out, the Obama Administration's formulation of a cross-domain deterrence strategy did nothing to prevent the DNC hack.[74] Similarly, the Obama Administration's economic and diplomatic responses to the attack failed to deter further Russian cyber aggression. Thus, Russia's reluctance to embrace cyber deterrence is motivated partly by doctrinal differences and partly by the belief that the theory has not worked in practice and is unlikely to do so in the future.

> ***"There is signficant Russian scepticism that cyberattacks can be meaningfully deterred."***

Finally, however, I also argue that the Russian government's contradictory stance on cyber deterrence is driven by the desire to maximise Russia's room for manoeuvre. Seen in this light, official opacity over Russia's offensive cyber policy is possibly a deliberate choice, designed to give the government maximum deniability and flexibility. This may reflect the fact that Russia's cyber capabilities are focused within its intelligence community, particularly the FSB.[75] These agencies are secretive and largely offense-oriented[76] and would likely be most opposed to cyber deterrence. From the FSB, GRU or SVR's perspective, accepting cyber deterrence could place unwanted restrictions on one of Russia's most effective power projection tools. For example, embracing cyber deterrence would mean agreeing that attacks on CNI would be off-limits. Many in Russian cyber circles could be loath to accept this, given that the threat of Russian attacks on CNI seems to be a highly effective way of

73 Maksim Krans, 'Кибероружие в арсенале НАТО', *Nezavisimoye Voennoye Obozreniye*, 21 June 2013

74 'White House International Strategy for Cyberspace', May 2011, p. 14

75 Sergey Sukhankin, 'The FSB: A Formidable Player in Russia's Information Security Domain', *Eurasia Daily Monitor*, Vol. 15, Issue. 46, 27 March 2018

76 Mark Galeotti, 'Putin's hydra: Inside Russia's intelligence services', *ECFR*, 11 May 2016

capturing Western attention and deterring NATO.[77]

Nevertheless, there are also sectors of the Russian foreign policy establishment, especially in the Foreign Ministry and academia, who have long stated that international agreements on information security and cyber 'norms' are essential to creating stability.[78] Such individuals worry about the effects of unrestricted information warfare practiced against Russia, as well as the danger of unintended escalation in cyberspace. This suggests that there is some disagreement between practitioners who want to exploit Russian cyber capabilities for immediate gain and strategists or diplomats who are concerned by cyber instability and feel that international regulation is in Russia's long-term interest. Given the increasing tempo of aggressive and offensive Russian cyber campaigns, it would seem that the practitioners and cyber 'hawks', are preeminent for now, to the detriment of those pushing for regulation.

Consequently, the key recommendation for Western policymakers is to **incentivise Russia to agree and ultimately accept the principles of cyber deterrence and cyber strategic stability**. Cyber deterrence is much more likely to be effective if Russia embraces the concept and this can be achieved through a combination of positive engagement and pressure. Thus, the West needs to harden its defences and make threats of punishment credible, while also remaining ready for dialogue. These goals can be achieved in two key ways.

Firstly, **Western governments should continue to refine and improve their own cyber posture.** This requires establishing credible red lines, such as a **joint declaration that attacks on CNI will incur a response**, coupled with a willingness to make good on the threat. Of course, it remains necessary to retain some ambiguity over what will elicit a response in order to avoid greenlighting all actions below the threshold. However, making clear that attacks on CNI are impermissible would not give Russia carte blanche to attack everything else. Similarly, **deterring Russia by denial remains vital to proving the long-term credibility of cyber deterrence**. Improving national and society wide cybersecurity will raise the cost of attacks, aiding attribution efforts as lesser actors are priced out. Similarly, capacity building in allied states can reduce the chances of cyber incidents spreading uncontrollably, while also raising the bar for attackers and aiding attribution. The FCO's Cyber Security Capacity Building Programme and NATO's efforts in Georgia[79] and Ukraine[80] are examples of how this can be done. By improving the credibility of deterrence, Western countries can incentivise Russia to accept the framework. Indeed, the FSB's decision to build a cyber deterrent implies that where the West leads, Russia will reluctantly follow.

> ***"Cyber deterrence is much more likely to be effective if Russia embraces the concept."***

Secondly, over the longer term, Western governments should **engage the Russian government to argue the case for cyber deterrence and address Russian objections**. Bilateral contacts and multilateral formats like the NATO-Russia Council or OSCE could serve as a springboard for these discussions, as well as reviving the stalled UN Group of Government Experts on Information Security.

77 Aubrey Allegretti, 'Russia could kill 'thousands' in UK power station attack, warns Defence Secretary', *Sky News*, 26 January 2018

78 Konstantin Peschanenko, 'Представители МО РФ о применимости норм и принципов международного права к военной деятельности в информационном пространстве', *Digital.Report*, 6 May 2015

79 'Substantial NATO-Georgia Package', NATO Factsheet

80 'Cybersecurity in Ukraine: National Strategy and international cooperation', *Global Forum on Cyber Expertise*, 7 June 2017

The ultimate aim of such discussions would be to produce an agreement modelled on the 2015 pact between the US and China. This agreement helped to reduce Chinese economic cyber espionage, as well as enabling regular high-level meetings and even the cooperative dismantling of 'some botnets and fake websites.'[81] Above all, it demonstrated that adversaries can negotiate restraining and mutually beneficial pacts on cyber security.[82]

Finally, if Russia and the West can agree to negotiate, **five fruitful areas for international agreement** spring to mind. These are:

1. Non-interference in political processes
2. Refraining from attacks on CNI
3. Refraining from attacks on the 'public core'[83] of the internet
4. Discussing common standards for attribution and
5. Publicly agreeing that cyberattacks on nuclear command and control are impermissible

Given the current political climate, such a process would have to start with Track 1.5 or 2 dialogue, focusing initially on those Russians who already support cyber regulation. However, this should be a long-term, multiyear effort aimed at bridging the gap between the two sides' positions. Moreover, the current impasse in Russia-West relations will not last forever and these negotiations should lay the groundwork for and capitalise on the next thaw in relations. Even a stable deterrence relationship is no substitute for a binding agreement on stabilisation and dialogue. Such an agreement can certainly be reached if the political will exists but it will require multiyear investment from both Russia and the West.[84]

81 Joseph B. M. Chua, '2015 U.S.-China Cyber Agreement: a new hope, or "the empire strikes back"?', Naval Postgraduate School, p.41

82 David E. Sanger, 'Chinese Curb Cyberattacks on U.S. Interests, Report Finds', New York Times, 20 June 2016

83 As defined by the Global Commission on the Stability of Cyberspace (GCSC), https://cyberstability.org/wp-content/uploads/2018/07/Definition-of-the-Public-Core-of-the-Internet.pdf

84 My heartfelt thanks to those who reviewed this paper and suggested improvements. Any remaining errors are of my own making.