The effect of emerging technologies on the offence-defence balance and deterrence: Cyber offence, lethal autonomous weapons systems and hypersonic glide vehicles.

Word Count: 10725

Date Submitted: 3rd September 2020

Abstract

In the wake of the Second World War and the rise of nuclear powers, national state security strategies for major powers indicate that creating strong deterrence through a build-up of capabilities is a model to ensure stability. The development, proliferation and operationalisation of new technologies by a state is therefore important to assess in their effect both on and off the battlefield at tactical, operational and strategic levels. This paper examines closely the effect of cyber offence, lethal autonomous weapons systems, and hypersonic glide vehicles on the offence-defence balance, determining their efficacy in lowering the cost of attacking and what sort of first strike impetus they provide for decision makers. Judging there to be an offence-dominance created by these emerging technologies with first move pressures, the paper then proceeds to scrutinise this resurgent offence advantage in its effect on deterrence and the feasibility of pursuing a deterrence posture. The most important conclusion drawn is that states will have a much harder time in relying on deterrence as cornerstones of their security as these new technologies are overwhelmingly useful in their current forms and their envisioned future systems in providing tactical and operational advantages for those choosing to attack. This in turn promotes instability and lowers the threshold for conflict between superpowers.

Table of Contents

Introduction

Multiple nation states, including all current superpowers, are explicit in their preference to maintain a posture of deterrence, presented either in their national security strategies or by their open build-up of a wide array of conventional capabilities.[1] Deterrence theory suggests that the prospect of nuclear war has prevented armed conflict between the great powers in the post WW2 era.[2] There have been periods of heightened tension, proxy warfare and 'face offs' between armed belligerents. Yet, major wars between Russia, China and the USA have not taken place. However, under this seemingly relatively secure umbrella of mutually assured destruction, although this is a contentious statement,[3] countries have felt emboldened to proceed with pursuing foreign policy goals which global rivals have found to be antagonistic and dangerous for their own security.

Decades of American primacy have created new impetus for states to upscale capabilities, both conventional and unconventional, to create a more favourable balance of power.[4] Rivals of the United States, namely China and Russia, have invested in cyber offence and hypersonic glide vehicles to challenge the West both below and above the threshold of war and those states are currently at an advantage in both areas. Autonomous weapons systems currently are unmanned measures for defence and commonplace in advanced militaries. Yet there is now scope for

[1] United Kingdom, Ministry of Defence, *National Security Strategy and Strategic Defence Review 2015*, (2015), assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/555607/2015_Strategic_Defence_and_Security_Review.pdf ; Japan, Japan Ministry of Defence, *Outline of the National Security Strategy*, (2015), www.mod.go.jp/e/publ/w_paper/pdf/2015/DOJ2015_2-2-1_web.pdf ; The People's Republic of China, State Council, *China's National Defense in the New Era*, (2019), english.www.gov.cn/archive/whitepaper/201907/24/content_WS5d3941ddc6d08408f502283d.html ; United States of America, The White House, *National Security Strategy of the United States of America*, (2017), www.whitehouse.gov/wpcontent/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf ; Pynnöniemi, K. (2018), pp. 240-256.
[2] Lieber, K.A. and Press, D.G. (2020), p.31.
[3] Lieber, K.A. and Press, D.G. (2006), p.8.
[4] Waltz, K. (1979).

autonomous offensive weapons systems with lethal measures such as planes, drones and missiles which forgo human control for a tactical advantage.[5]

This analysis will assert that the emergence of new technologies, namely lethal autonomous weapons systems (LAWS), cyber offence capabilities and hypersonic glide vehicles (HGVs), all applied for military means in the 21st century has created an era of offence dominance. There is now a revolution in military affairs similar to the one experienced in the 1930s with combined arms mechanised manoeuvre warfare.[6] These technologies, applied in tandem with existing conventional and unconventional capabilities, allow nation states to be far more aggressive in pursuing policy goals, including escalation into acts of war. The speed of response for these three different technologies achieves major tactical and operational benefits for any state but these benefits are bought through the cost of losing centralised strategic control.

I will demonstrate in the dissertation that this combination of LAWS, cyber offence and HGVs all contribute to this resurgence of offence as cyber defence, missile defence and the legal and ethical international frameworks and agreements for LAWS struggle to catch up in effectiveness.[7] This will be done through extrapolating an assessment of the current and future worth of these emerging technologies through contemporary scholarship and the user state's own views.

Hypothesis

[5] Garcia, D. (2018).
[6] Citino, R.M. (2005).
[7] Rydell, R. (2020) ; Saltzman (2013) ; United States of America, U.S. Department of Defense, *2019 Missile Defense Review*, (2019).

The main conclusion in this work is that this offence dominance is dangerous for international state stability due to the increased impotence of deterrence and the difficulty in signalling a credible deterrence posture. This resurgent age of offence advantage provides the evidence to empower hawks and a decision maker does not have to be hawkish themselves to be hostage to its imperatives. This paper will argue that major powers are both under first strike pressures as insistent as any time in the nuclear age and entering into a period where there are 'use it or lose it' capabilities which are time sensitive in their efficacy.

The paper asserts there is cause for concern in that all of these new technologies have off ramps to deescalate situations, particularly deniability of their use, yet the practice of these capabilities in tandem with one another might prove too overwhelming to even the most resistant dove decision maker. If there is this imperfect escalation control, then tactical and operational benefits might end up undermining strategy and policy, particularly the status quo of relative stability in the previous seven decades. Clausewitz's observation that war's nature is to escalate once underway is pertinent then as first move advantages provided by these new technologies might limit a conflict due to the potential speed of success, which might otherwise have been total in its scope.[8] This potential for a fast and successful conflict is a seductive prospect for decision makers.

The paper first looks at the credibility of the emerging technologies and their potential at tactical and operational levels to form an era of offence dominance, and establishes that there are first move pressures. It then moves onto exploring what effect these new technologies have on deterrence as a concept and the utility of states' postures of deterrence. Finally, it will examine what the technologies

[8] Clausewitz, *On War*, tr. Howard and Paret, p.77.

therefore mean for state stability and brings forward several policy recommendations for major powers operating with these technologies and those opposed to them.

Chapter 1: Credibility and potential of the emerging technologies

It is imperative to begin this dissertation by establishing the specifications, abilities and credibility of cyber offence, lethal autonomous weapons systems and hypersonic glide vehicles in their current form.

Cyber offence

Cyber offence can be conducted through several methods, which Thomas Rid claims are attempts to perform acts of "sabotage, espionage and subversion".[9] Many of the tools originate and are operated from the criminal sector with help and shielding from their host governments.[10] Distributed denial-of-service (DDOS) is a particularly low level and common form which involves overloading servers with requests to crash digital sites. Malware which includes viruses, worms, spyware and ransomware, is another common form of cyber-attack. An important element of cyber offence are exploits or vulnerabilities within systems and specifically zero-day exploits which are pre-identified loopholes and gaps within systems which can be exploited by adversaries and actors from the launch of software or servers, and are often used in tandem with rootkits. A clear example of this in action was the Stuxnet computer worm which caused major damage to Iranian nuclear centrifuges, an act of sabotage independent from any conventional operations.[11] The Stuxnet attack was both an exploit of Iranian cyber vulnerability and also in the domain of Advanced Persistent Threats, which is a process of lurking and collecting information for an extended period of time, often subsequently attributed to states.[12]

[9] Rid, T. (2012), p.5.
[10] Sofaer, A. and Goodman, S. (2001).
[11] Langner R. (2013). 'Stuxnet's Secret Twin'. *Foreign Policy.* www.foreignpolicy.com/articles/2013/11/19/stuxnets_secret_twin_iran_nukes_cyber_attack.

[12] Nakashima, E. and Warrick, J. (2012), "Stuxnet was work of U.S. and Israeli experts, officials say", *The Washington Post*. www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html

Cyber offence as a set of tools has been gaining more and more credibility with major and highly publicised instances of states and key private sector institutions being subjected to cyberattacks with geopolitical interests. The 2007 cyber-attacks on Estonia crippled its government and the financial systems there due to a heavy reliance on digital based services. It was likely spawned from a government decision to relocate a Soviet era Bronze Soldier statue to a military cemetery from the city centre of Tallinn. These series of attacks were in conjunction with pro-Russian riots in Tallinn and economic sanctions from Russia against Estonia.[13] Cyber offence here is credible as the Russian government denied being the originator of the attacks and the criminal sector was blamed, yet cyber offence gained a strategic advantage for Russia. Estonia was harmed through internal political and economic unrest without Russia suffering a diplomatic penalty with other states. Other examples of cyberattacks made public were the Iranian retaliation for Stuxnet against American banks and Saudi Aramco in 2012,[14] and the Sands Casino in 2014.[15] The North Korean hacks against Sony Pictures in 2014, suggested as an attempt to deter the upcoming release of the film *The Interview* by the studio, is an example of the intersection cyber offence creates between geopolitics, soft power and the private sector. Cyber offence is clearly credible enough of a tool to warrant serious discussion and fear on its potency as NATO for example has warranted that a cyber-attack is worthy for Article 5 to be invoked.[16]

Lethal Autonomous Weapons Systems

[13] Maigre, M. (2015), p.4.
[14] Gorman, S and Barnes, J.E. (2012), "Iran Blamed for Cyber Attacks", *The Wall Street Journal*. www.wsj.com/articles/SB10000872396390444657804578052931555576700
[15] Elgin, B. and Riley, M. (2014). "Now at the Sands Casino: An Iranian Hacker in Every Server", *Bloomberg*. www.bloomberg.com/news/articles/2014-12-11/iranian-hackers-hit-sheldon-adelsons-sands-casino-in-las-vegas
[16] NATO, (2019). 'NATO will defend itself', *NATO*. www.nato.int/cps/en/natohq/news_168435.htm

LAWS currently exist mainly in defensive forms such as the US Navy's MK-15 Phalanx anti-aerial weapons system, or the Russian active protective system Arena, or the Israeli missile defence Iron Dome system, which all have the capability of targeting and firing without supervision from humans.[17] They are programmed beforehand by humans and operate within those constraints. The Phalanx system for example is constrained in both its placement, either on land or on ship decks, and the types of targets it can engage. It does not have the ability to 'learn', via machine learning, targeting of new threats nor the ability to adapt to more complicated situations. These fully autonomous learning systems are still conceptual. The Phalanx provides defence capability 'against anti-ship missiles (ASM), aircraft and littoral warfare threats that have penetrated other fleet defenses' and can 'counter small high-speed surface craft, aircraft, helicopters and unmanned aerial systems (UAS).' This is done through its ability 'of autonomously performing its own search, detect, evaluation, track, engage and kill assessment functions'.[18] The Phalanx system's current capabilities show both its limitations in its current form but also its potency as a battlefield weapon. The lack of human supervision beyond the initial construction and programming has prompted multiple legal and ethical questions over accountability, proportionality of response and targeting. In their current defensive formats in non-complex environments, these questions are not sources of conflict between proponents and opponents to autonomous technology. However, projects like the Israeli Harpy, the autonomous unmanned aerial vehicle designed to seek out and destroy unfriendly radar emitters, are a greater cause for ethical concern. This technology, like the Phalanx, is programmed within its certain

[17] Center for Security Policy and VanNess, A. (2013), pp.24-27.
[18] US Navy, (2019), *MK 15 - Phalanx Close-In Weapon System (CIWS)*. www.navy.mil/Resources/Fact-Files/Display-FactFiles/Article/2167831/mk-15-phalanx-close-in-weapon-system-ciws/

constraints, without artificial intelligence learning. This level of programming is effective in that it cuts out human error due to its quality of design and is far less able to operate outside of its purview and law of armed conflict.[19] There is deep potential however for autonomous defensive and offensive systems to become more than battlefield auxiliaries and instead replace soldiers who are in harm's way. The problem is discerning combatants within the 21st century where combatants might be misrepresented as civilians and vice versa. Roff uses the example that LAWS 'must be able to, with sufficient ability, discern the difference between, say, an Afghani farmer wandering the countryside tending to his flocks and openly wearing an AK47 across his shoulders and an Afghani Taliban insurgent wearing generally the same clothing and openly carrying arms'.[20] Roff observes that the answer by proponents of LAWS to these conundrums in attempting to operate LAWS in accordance with the LOAC and rules of engagement depends on the programming of the software. There is therefore great scope for programming to be more effective in executing military purposes but that loss of accountability might be far more problematic in terms of maintaining a centralised control. LAWS have earned their reputation and credibility in defensive sectors, yet their potential for swiftly winning wars lies in offensive operations.

Hypersonic glide vehicles

Both Russia and China have publicly revealed their hypersonic glide vehicles which are the Avangard and the DZ-ZF respectively. These can both deliver nuclear payloads alongside conventional warheads. The Avangard is stated to operate at

[19] Roff, H.M. (2014), pp.212-213.
[20] Ibid, p.213.

speeds of Mach 20,[21] while the DZ-ZF is estimated to be between speeds of Mach 5 to Mach 10.[22] The claims by Russian state sources that the Avangard missile, being able to perform high speed horizontal and vertical evasion manoeuvres, is not capable of being neutralised by any missile defence system are a major cause for concern for other major powers. This level of battlefield prowess would allow Russia to target any stationary or moving target on the globe within minutes. Decision makers in the United States have noted the importance and danger HGVs bring to combat, although there might be some scepticism over Russian and Chinese claims of the Avangard and DZ-ZF's actual speeds and manoeuvrability. They have both ramped up successful testing of their own HGV systems in development,[23] clearly judging that HGV as a capability is desirable and necessary for their own security. American lawmakers have been gathering increasing consensus and been making pushes for funding for development for HGVs and defence against them in Congress.[24]

Chapter 2: Offence dominance and first move pressures

Part of the importance of establishing the capability and credibility of these technologies is to examine them in tandem with their current antagonistic counterparts, namely cyber defence, the lack of international consensus over legality and ethics surrounding LAWS, and missile defence. This paper aims to establish that

[21] CSIS, Missile Threat, *Avangard*, (2020). missilethreat.csis.org/missile/avangard/
[22] Gady, F. (2016), 'China Tests New Weapon Capable of Breaching US Missile Defense Systems', *The Diplomat*. thediplomat.com/2016/04/china-tests-new-weapon-capable-of-breaching-u-s-missile-defense-systems/
[23] Reif, K. and Burgos, S. (2020), 'Pentagon Tests Hypersonic Glide Body', *Arms Control Association*. www.armscontrol.org/act/2020-04/news/pentagon-tests-hypersonic-glide-body
[24] Federation of American Scientists, Congressional Research Service, *Conventional Prompt Global Strike and Long Range Ballistic Missiles: Background and Issues*, (2020). fas.org/sgp/crs/nuke/R41464.pdf

there is a definitive offence dominance with these emerging technologies, particularly due their first strike potential. There are clear advantages of speed of operation and response within these technologies, yet might come as a trade off against centralised control of operations and strategy. For the purpose of clarity, Glaser and Kaufmann's definition of offence-defence balance is the most appropriate for this essay: "We prefer to define the offense-defense balance as the ratio of the cost of the forces the attacker requires to take territory to the cost of the forces the defender has deployed".[25]

Cyber offence-defence balance

Deputy Secretary of Defense William Lynn wrote in 2010 that "In cyberspace, the offense has the upper hand".[26] The offence-defence balance within cyber is potentially the most pronounced and public at this moment in time. This paper somewhat agrees with Hersh's definition of cyber war as the "penetration of foreign networks for the purpose of disrupting or dismantling other networks, and making them inoperable".[27] Locatelli uses this definition to assess the offence-defence balance within cyberspace in a purely state on state contest, 'actions perpetrated by and aimed at state actors'.[28] He comes to three conclusions:

1) There is a centrality of defence vulnerabilities, as it is unfeasible to disconnect computers from networks while also impossible to rule out weaknesses within software.

[25] Glaser, C.L and Kaufmann, C. (1998).
[26] Lynn, W.J. (2010), p.98
[27] Hersh, S. (2010), 'The Online Threat: Should We Be Worried about Cyber War?', *The New Yorker*. www.newyorker.com/magazine/2010/11/01/the-online-threat
[28] Locatelli, A. (2013), p.8.

2) Progress in offence is faster than defence due to the slower technological evolution of defence. The offence is the side to find flaws in defence to then be plugged up by cyber defence with better software.
3) Attribution is difficult in cyber defence. There can be a large geographic difference with cyber attackers compared to the defender and also small numbers of personnel are needed to orchestrate a cyber-attack. It is much easier for a host government to deny that the cyber attackers are coordinating with their government with fewer cyber attackers.[29]

There are implications for first strike incentives for cyber offence here. Cyber offence cannot succeed without testing the software and systems of the cyberspace controlled by adversaries, so there is an impetus to constantly attack and penetrate hostile systems to keep any strategic edge. There is therefore huge potential for instability as first strikes within cyberspace do not have the same lethal implications that conventional first strikes do have. If gaps are identified in the defence, then exploiting those gaps is incentivised as exploits might not be effective if those gaps are then patched with newer software. Although this might then seem to be acts below what constitute warfare, cyber offence's value has been shown in its capability in assisting and paving the way for successful military operations. Operation Orchard in 2007 involved a pre-emptive cyberattack by Israeli operators into Syrian monitoring and air defences, which then allowed Israeli fighter jets to bomb a potential nuclear reactor in Syria itself.[30] Saltzman, like Locatelli, looks at the costs between cyber offence and defence and that a combined cyber-conventional force

[29] Ibid, p.8-9.
[30] Saltzman, I. (2013), p.40.

operation like the Israeli attack on Syria is a relatively low-cost alternative in minimising risks of taking offensive action.[31]

The reluctance of certain states and alliances, namely NATO, to engage in outright cyber offence, only heightens this disparity between the effective results seen in cyberattacks (Estonia 2007, Syria 2007) and the problems with plugging the gaps in cyber defence. This is due to retroactively tightening cyber security after a major attack is the nature of cyber defence itself, a reactive heightening of capability to try to neutralise cyber offence. This is all done with a financial cost, which can and mostly is at a large imbalance with the cost of the offence to precipitate such damage. Syria 2007 is especially relevant when weighing up the cost of the cyber offence and fighter jet operation with the now defunct air defence software, and the potential nuclear facility's destruction.

Schneider's assessment into the capability-vulnerability paradox is useful in analysing cyber offence's dominance, with her focus on the information revolution within warfare. The heavy reliance on digitally held information to give militaries a technological edge has made them "extremely vulnerable because of increasing dependencies on information".[32] Secretary Lynn has argued that "information technology enables almost everything the military does" and that it is a "national strategic asset".[33] Therefore, if military powers are able to exert power and force because of their functioning digital and cyberspheres, the first strike incentives must be much greater as it is all more vital to adversaries to target that reliance if it is vulnerable and open to cyberattack. Schneider agrees with this assessment finding that the "increases in highly centralised networks and the proliferation of digital

[31] Ibid, p.58.
[32] Schneider, J. (2019), p.842.
[33] Lynn, W.J. (2010), p.98

vulnerabilities within civilian infrastructure, combined with a continued belief in offense dominance, could increase incentives for first strike over time".[34] The spectacular success of Stuxnet, Estonia 2007 and Syria 2007 has at least demonstrated cyber offence's capability. The limited casualties caused and taken to achieve strategic goals might then seem enticing to decision makers, whether the offence dominance is in reality as pronounced as it appears.

Slayton enriches the analysis over cyber offence-defence balance by adding the high variability of skills which differ between cyber offence and cyber defence, instead of just looking at the balance in terms of cost alone. She estimates the value of the Stuxnet program including all labour to have been far greater in cost than the unsuccessful defence and subsequent damages to the Iranian nuclear program.[35] Slayton's analysis into the costs of Stuxnet are then pertinent in looking at the current perception of offence-defence balance with decision makers, rather than the actual reality. Stuxnet can be seen to have been an expensive but successful investment for the long term as Slayton argues that the now "increased suspicion and paranoia will take a significant long -term toll on the Iranian nuclear project". It can be compared to the US nuclear program which "incurred similar damage in the wake of allegations of espionage at Los Alamos National Laboratory".[36] There is consensus amongst states engaging in cyber offence that there is an offence dominance, backed up by the publicity of large scale cyberattacks.

Lethal autonomous weapons systems offence-defence balance

There is an offence-dominance in the field of LAWS in two separate senses: the first is the arms racing of states with technical upgrades and pioneering new systems of

[34] Schneider, J. (2019), p.842.
[35] Slayton, R. (2017), p.98.
[36] Ibid, p.106.

LAWS to effectively achieve greater operational speed than opponents. This ultimately falls into offence category as machines, which can operate and execute their objectives faster than their enemies with fewer losses of friendly life, are likely to be offensive in nature. This is because LAWS substitute the human element of the military and place those personnel out of the firing line. This attempt to achieve operational speed has been predicted as the key factor in the success of LAWS. Artificial intelligence in LAWS of the future with decision making algorithms would be able to out compete and execute faster operations than human pilots or operators or indeed remotely controlled technologies.[37] The race for operational speed which is only achievable through machine learning, decision making algorithms and a hands off approach from human supervisors, is pressurising enough for decision makers to invest and build up LAWS capabilities faster and better than great power rivals.

The U.S. Department of Defense demonstration of 103 *Perdix* micro drones, which are capable of "advanced swarm behaviours such as collective decision-making, adaptive formation flying and self-healing",[38] is cited by Altmann and Sauer as an important example. A modern technologically advanced military like the United States sees the future battlefield as requiring more LAWS basing offence on sensors and artificial intelligence to overwhelm human piloted and remotely controlled technologies to achieve "superior unmanned air-to-ground *and* air-to-air capabilities across the board".[39] The overall cost with projected 3D printed units and deployment in large quantities from far fewer manned aircraft points to a much cheaper cost of conducting warfare, both in body bags and monetary value. The reliance on sensors,

[37] Altmann, J. and Sauer, F. (2017).
[38]United States, U.S. Department of Defense, ''Department of Defense Announces Successful Micro-Drone Demonstration", (2017), www.defense.gov/Newsroom/Releases/Release/Article/1044811/department-of-defense-announces-successful-micro-drone-demonstration/
[39] Altmann, J. and Sauer, F. (2017), p.123.

digital signals in the form of code and artificial intelligence executing lethal decisions makes it all the harder for a defence to disrupt communications or take advantage of those communications, whereas human communications at the moment can be a vulnerability for a military operation.

The second element of LAWS offence dominance is down to the lack of success of campaigners against the roll out of machines which can make decisions on their own with lethal consequences. To put it simply, major states at this point are developing LAWS with a vigour that a concerted diplomatic effort to limit their use could not hope to match. There is too much enthusiasm and success already with LAWS to halt their development even as legal and ethical questions are posed and not yet definitively answered, as norms and rules of engagement have not been established through combat. Arms control is difficult, especially with technology like LAWS which has deep and extremely consequential potential. The United Nations has found in the past with its Secretaries-General that arms control and disarmament initiatives have been challenging processes where consensus is almost always never achieved.[40] The United Nations Convention on Certain Conventional Weapons has been debating autonomous weapons systems in a discussion surrounding the proposed restriction of LAWS, yet after six years of discussion, there is still ambiguity and lack of consensus over the definition of LAWS. Haas and Fischer point out that the CCW requires consensus as part of its principles on forming treaties and this mechanic will complicate attempts to form an agreement.[41] The United States' policy directive on "Autonomy in Weapons Systems" in 2012 is stunted at best and only is applicable on a national level, with a timeframe of ten years. LAWS with a human in control for lethal functions at this point in time will not require human supervision by

[40] Rydell, R. (2020).
[41] Haas, M.C. and Fischer, S. (2017), p.296.

2022.[42] In this way, LAWS are seemingly unopposed in their development and there appear to be clear avenues for proliferation of their current numbers and technological advancement in the future. Nation states, without a consensus over non-proliferation of LAWS, will look to securing themselves by developing offensive machine speed LAWS. This is a neorealist view, which has serious implications for how to deter a country without human supervision over lethal functions.[43] The first strike advantages will become clearer as the technology advances if the current interpretation is that operational speed will be the deciding factor for the success of a lethal autonomous weapons system of the future.

Hypersonic glide vehicles: missile offence-defence balance

Hypersonic glide vehicles are one component of overall offence-defence balance for missile technology, another capability which missile defence systems have to guard against. HGVs as a technology have been developed in response to far more sophisticated ballistic missile defences established by the United States during their period of unipolar hegemony. These defences ultimately are more deterrence by denial in nature and aimed at rogue states like North Korean and Iran, rather than superpowers of Russia and China.[44] However, HGV survivability from launch to delivery of the payload is precisely the sort of credible deterrent desired by Russia, China and the United States to maintain stability. Karako and Williams acknowledge the sheer numbers of ICBMs possessed by Russia and China with nuclear capabilities makes it unlikely that even the most sophisticated homeland missile defences could neutralise them.[45]

[42] United States, U.S. Department of Defense. "Department of Defense directive 3000.09: The role of autonomy in weapon systems". (2012). fas.org/irp/doddir/dod/d3000_09.pdf
[43] Mearsheimer, J (2001) ; Waltz, K (1979).
[44] Karako, T. and Williams, I. (2017), p.19-20.
[45] Ibid, p.20.

Missile defences are both expensive and do not assure themselves of any ready degree of success at this moment. The September 2019 Abqaiq-Khurais attack on Saudi Aramco facilities is a key example of the rampant overspend of missile defence, which still failed to protect the oil refineries. The Saudis were equipped with the MIM-104 Patriot surface-to-air missile defence system, and are reported to spend $180 million per year on defence, “yet they were not able to attrite, much less stop, a cruise missile attack on one of their most critical facilities”.[46] Low flying cruise missiles and swarms of inexpensive drones were successful in halving Saudi Arabia’s oil production. This attack shows the financial difficulty in making missile defence successful as expensive systems like the Patriot are flawed and vulnerable to far cheaper methods of warfare. There is scepticism over the efficacy of the Ground Based Midcourse Defense system, the United States’ homeland missile defence against long range ballistic missiles through the use of interceptors. Grego scrutinises the system, claiming it is dated, expensive and unable to counter the advanced threats posed by China and Russia.[47] This clearly swings the balance of missiles towards offence and adding HGVs only compounds this problem.

HGVs do not rely on mass of numbers to swarm a missile defence system, instead focusing on high altitudes, extreme speeds and exceptional manoeuvrability to deliver payloads. These therefore are tempting for decision makers as instead of launching half a missile arsenal, there need only be limited quantities of HGVs to achieve an effective first strike on any target of choice. Decision makers might also be persuaded to engage in first strikes with HGVs due to the unlikeliness in triggering mutually assured destruction with a nuclear armed state. The kinetic energy alone, due to the speeds of Mach 9 for example making any chemical agent

[46] Oelrich, I. (2020), p.44.
[47] Grego, L. (2018).

or explosive on top of the HGV almost superfluous in its damage yield (although accuracy would be harder to maintain),[48] would still have a sizable impact akin to nuclear devices but without the cultural or social stigma associated with nuclear warheads.[49]

With these three technologies assessed in their present forms and the future potential of LAWS, there are incentives for decision makers and states to invest in all three technologies for the tactical and operational advantages they currently give and will be capable of in the future. Cyber offence relies on constant pressure on the defence to demonstrate that advantage and it has the dual quality of being able to carry out operations to achieve strategic goals in 'peacetime' such as Estonia 2007 and compliment conventional operations in armed conflict, with the example of Syria 2007. LAWS have the most potential and the current rhetoric and testing, especially from the United States, indicates that warfare of the future will feature LAWS heavily in offensive actions. This is due to the predicted superior speeds of operation, machine speeds far greater than humans or remotely controlled capabilities could ever achieve.[50] The operational velocity and evasiveness of HGVs from launch to delivery of the payload makes them the next step for major powers in mitigating missile defence. The heavy investment from all the current superpowers shows their future prowess in targeted strikes. There is no foreseen hypersonic missile defence until the middle of the decade at the earliest.[51] These all are therefore operationally useful technologies and will give any users tactical and operational benefits both on

[48] Oelrich, I. (2020), p. 42-43.
[49] See Tannenwald, N. (1999). for the difficulties on the cultural objections to nuclear power.
[50] Horowitz, M.C. (2019), p.769.
[51] United States, U.S. Department of Defense, "Media Availability With Deputy Secretary Shanahan and Under Secretary of Defense Griffin at NDIA Hypersonics Senior Executive Series", (2018). www.defense.gov/Newsroom/Transcripts/Transcript/Article/1713396/media-availability-with-deputy-secretary-shanahan-and-under-secretary-of-defens/

and off the battlefield, yet their existence and future proliferation in quantity and usage has severe implications for deterrence and stability.

Chapter 3: Deterrence

The key questions for states therefore which currently maintain postures of deterrence are can one actually deter the proliferation and use of these technologies, both above and below the threshold of warfare, and can a state still maintain a posture of deterrence? This section builds on the initial explorations of offence dominance and first strike advantages, and focuses on the nuclear postures, nuclear stalemate and counterforce, the stability-instability paradox, escalation control, the potential difficulties of credible signalling and finally deniability.

Nuclear postures

One of the key problems facing deterrence is the distinct differences in how states treat aggression between conventional conflict and nuclear threats. Nuclear armed states mostly have a stated stance on engaging in first or second nuclear strikes. China, out of the nuclear armed superpowers, has been the clearest for a long time on its policy on use of nuclear weapons, that they are for retaliatory second strikes only in the case of self-defence.[52] This stance forms its 'minimum deterrence' doctrine.[53] This defensive posture and exclusivity of the usage of nuclear weapons only in response to nuclear attacks is limiting in nature in how China can coerce enemies and rivals through its nuclear strategy. This no-first-use policy invites opponents to challenge China in conventional means if these opponents do not plan

[52] People's Republic of China, Ministry of Foreign Affairs of the People's Republic of China, 'Position Paper of the People's Republic of China at the 66th Session of the united Nations General Assembly', (2011). www.fmprc.gov.cn/eng/zxxx/t857763.html.
[53] Pan, Z. (2018), p.117.

to escalate past the nuclear threshold. This lack of coercion has led to calls within China to expand their posture into the same of the United States and Russia. This would lower the nuclear deterrence threshold, meaning that conventional threats might be enough to warrant nuclear strikes.[54] Russia maintains both a retaliatory second strike posture and simultaneously the right to retaliate in a nuclear manner against a conventional attack which threatens the Russian state.[55] This is almost a no-first-use policy and warrants nuclear use if the Russian state is under an existential nuclear or conventional attack. Both China and Russia have indicated that mutually assured destruction is secured under their deterrence postures. The United States' similarly is half-committed to a no-first-use policy but does indicate that low-yield nuclear options will be contemplated against conventional threats aimed at their own nuclear systems.[56] All three superpowers in this way are steadfast in appearing that they want to not escalate to nuclear before the other. Waging a conventional war does still hold the risk that overstep in use of force and targeting, like the potential destruction of any of the state's political centres and command, will warrant a nuclear response.

Nuclear stalemate and counterforce

Therefore, it is important when examining the viability of deterrence to determine if this nuclear stalemate is still functional as a pillar of security. One indication that the nuclear stalemate is not as secure as the current postures would hopefully signpost to the world is that all these superpowers still arms race and proliferate their capabilities to varying degrees, shown especially through the emergence of these

[54] Lieber, K.A. and Press, D.G. (2020), p.117.
[55] Stowe-Thurston, A. and Korda, M. and Kristensen, H.M. (2018), "Putin Deepens Confusion About Russian Nuclear Policy", *Russia Matters*. www.russiamatters.org/analysis/putin-deepens-confusion-about-russian-nuclear-policy
[56] United States, U.S. Department of Defense, 'Nuclear Posture Review 2018), (2018). dod.defense.gov/News/SpecialReports/2018NuclearPostureReview.aspx

three technologies. Lieber and Press focus on the important question of why do states continue to increase their arsenals and wide array of forces when they supposedly have a secure second strike? Their answer is that some states are constantly trying to reverse the nuclear stalemate while others are attempting to maintain it.[57] A stalemate reversal is carried out through creating extremely accurate counterforce capabilities. The development of hypersonic glide vehicles might indicate that there has been a real fear amongst the superpowers that missile defence might have been more capable than anticipated in all major powers' homelands, that intelligence, reconnaissance and targeting might have all improved to such a degree that a second-strike luxury was at risk.

A survivable arsenal is required to undertake a second strike and decision makers in the three nuclear armed superpowers have decided to invest in HGVs perhaps thereby indicating that manoeuvrability and operational speed are now the required criteria to actually deliver a nuclear payload. HGVs in this case could strengthen nuclear deterrence through reaffirming the stalemate which Lieber and Press argue is waning. They have the added benefit, being re-entry vehicles of existing outside the jurisdiction of arms control agreements, allowing a development of real quantity.[58] Conversely, HGVs, alongside other advances in intelligence, accuracy and targeting, have the potential to embolden decision makers into making disarming first strikes, which has serious implications for deterrence postures. Air and land based nuclear warhead delivery systems might be under threat in this manner, empowering states which rely on submarines for nuclear deterrence. As counterforce measures, HGV stated capabilities allow them to evade missile defence systems and anti-access area denial weapons, making nuclear arsenals at risk in their survival. A

[57] Lieber, K.A. and Press, D.G. (2020), p.66-93.
[58] Williams, H. (2019), p.796.

key part of this is the perception of HGV abilities, a topic which shall be explored later in the paper. The production of a technology with no obvious means to defend against it might make a decision maker extremely confident in aggression.[59]

"The stability-instability paradox"

If nation states accept that their mutually assured destruction is secure, that there is a nuclear stalemate, then can that nuclear escalation threat deter conventional attacks? This is exaggerated by stated no-first-use policies which raise the nuclear threshold considerably. Part of the reasoning for why this paper argues that deterrence is weakened with the presence of these new technologies is due to the "stability-instability paradox". Nuclear armed powers in competition, knowing that mutual annihilation is a definitive prospect, instead must engage in more limited forms of geo-politicking and limited armed conflict to achieve strategic aims. Liddell Hart argued in 1954 that "to the extent that the H bomb reduces the likelihood of full-scale war, it increases the possibility of limited war pursued by widespread local aggression".[60] The more certain that nuclear deterrence is secure, the more likely the instability at levels lower than the nuclear threshold.[61] Two examples of the "stability-instability paradox" working in reality is the border tensions and conflicts between India and Pakistan, typically over the disputed region of Kashmir, and recently the Sino-Indian clashes over the LAC in eastern Ladakh. Kashmiri separatist group Jaish-e-Mohammed carried out a suicide bomb attack on Indian military personnel which lead to in Indian bombing runs over Kashmir and ventured into Pakistani airspace, resulting in casualties for the separatists and an Indian pilot being downed

[59] Ibid, p.798.
[60] Liddell Hart, B.H. (1960), p.23. Initially published in 1954.
[61] Lieber, K.A. and Press, D.G. (2020), p.95.

by Pakistani forces.[62] The instability in the region has been present since the partition at both states' independence, predating their nuclear capabilities, yet has not resulted in a nuclear exchange in all their tensions, disputes and armed conflicts. The Ladakh skirmishes involved melee fighting between two superpowers in their own right with nuclear capabilities.[63] Again this is a case of instability and opportunism to achieve strategic goals without escalating to a state of warfare. These limited conflicts showcase the "stability-instability paradox" with nuclear powers still engaging with aggressive, inflammatory foreign policy when they deem it necessary, despite the potential of nuclear war, demonstrating a failure in deterrence. In this manner, cyber offence and, to a lesser extent, LAWS can be applied to this unstable limited conflict area whereby deterring states from attempting to attain their objectives is difficult.

Difficulties of deterrence with the "stability-instability paradox"

Cyber offence, out of the three, is the most suited technology for decision makers to engage in this testing of another state's mettle in upholding their own deterrence postures. There is a near universal muddled view of cyberattacks, where to gauge the severity of the consequences surrounding a cyberattack, including use of force and targeting, invites debate.[64] This ability to deny and bring about confusion and doubt is a key part of any cyber aggressor's toolkit and will be explored later. Rid's assertion, cited earlier, that cyberattacks are "sabotage, espionage and subversion", all three being implements used in peacetime as well as wartime, demonstrate the acceptance by the international community of cyber offence as a mainstay of

[62] Slater, J. and Constable, P. (2019), "Pakistan captures Indian pilot after shooting down aircraft, escalating hostilities", *Washington Post*. www.washingtonpost.com/world/asia_pacific/pakistan-says-it-has-shot-down-two-indian-jets-in-its-airspace/2019/02/27/054461a2-3a5b-11e9-a2cd-307b06d0257b_story.html
[63] Biswas, S. (2020), "India-China clash: 20 Indian troops killed in Ladakh fighting". *BBC News*. www.bbc.co.uk/news/world-asia-53061476
[64] Edwards, B., Furnas, A., Forrest, S., and Axelrod, R. (2017), pp.2825-2830.

achieving strategic goals.[65] NATO's designation of a cyberattack as an offence worthy enough to invoke Article 5,[66] an example used earlier, therefore appears to be mere posturing, and not sufficient to be an effective form of deterrence. The article itself has only been invoked once during the history of the Alliance and collective defence as a concept is extremely hard to prove credibility, especially if one takes a neorealist view. NATO as an alliance exists in a multipolar world where states, even those on the same side of balancing, have differing strategic objectives.[67]

Legally a state can defend itself from accusations of cyberattacks inflicting actual harm and constituting an act of aggression through publicly subscribing to an instrument-based approach over use of force. In international law, "the instrument-based approach holds that only traditional weapons with physical characteristics can constitute an armed force required to carry out armed attacks".[68] Therefore, it is much harder to deter a cyberattack if a state knows that a greater response in retaliation to cyber offence, which would be legally considered below the threshold of armed conflict, would then paint the aggrieved state as the instigator of conflict.

There is yet more freedom for states to engage in cyberattacks without incurring severe responses despite the severe penalties a cyberattack can inflict on a state's critical infrastructure. The vulnerabilities created with a state's reliance on information and digital access has shown to be extremely exploitable by cyber offence. The ransomware worm "WannaCry" which targeted the National Health Service in 2017, locking health professionals and NHS staff out of their computers unless they paid out Bitcoin resulted in serious delays in delivering medical treatment

[65] Rid, T. (2012), p.5.
[66] NATO, (2019). 'NATO will defend itself', *NATO*. www.nato.int/cps/en/natohq/news_168435.htm
[67] Waltz, K. (1979), p.111.
[68] Sheng, L. (2013), p.179.

in hospitals while surgeries and general practitioners were forced to lock their doors and ceased to treat patients.[69] This sudden and seemingly technologically unimpressive worm managed to shut down a third of the United Kingdom's healthcare trusts and cost the health service £92 million.[70] A larger attack in 2015 at Anthem Blue Cross Insurance System resulted in 78 million medical records being stolen.[71] Health as a sector is "one of the most vulnerable to cyberattacks, yet it has chronically underinvested in cyber resilience".[72] 46 major financial institutions in the United States in 2016 were hit with a large scale DDOS attack flooding target servers with traffic and preventing their use, with the most noticeably harmed bank being JPMorgan Chase.[73]

The securitisation of areas previously not visibly linked to a state's defence, namely health and finance, is important as all of these areas are susceptible to cyber offence. This has the implication that deterring cyberattacks will only get harder in the future because of the cost imbalance between offence and defence. As the range of areas vulnerable to cyber offence increases because of securitisation, the much greater amount of money will be needed to invest in cyber security across all those platforms to generate resilience. If citizens' health and prosperity is negatively affected by failing to stop cyberattacks, that is a failure of deterrence. In terms of strategic balance, failure to deter cyberattacks allows states weaker in terms of relative power and criminal groups or terrorists to acquire better hacking technologies, emboldened by success. In contrast to this, the reliance of more

[69] Clarke, R. and Youngstein, T. (2017), pp.409-411.
[70] Field, M. (2018), "WannaCry cyber attack cost the NHS £92m as 19,000 appointments cancelled", *The Telegraph*. www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled/
[71] BBC News, (2018). 'Singapore personal data hack hits 1.5m, health authority says', *BBC News*. www.bbc.co.uk/news/world-asia-44900507
[72] Ghafur, S., Kristensen, S., Honeyford,K. (2019), p.98.
[73] Tariq, N. (2018).

technologically advanced states on the digital sphere leaves them even more vulnerable to cyber offence.[74] Initial success of cyber offence can therefore snowball into much more potent future successes.

LAWS also have the potential to be utilised by states within this "stability-instability paradox" to stretch deterrence of states. UCAVs have a particularly bright future here in their capability to stretch deterrence under the safe nuclear umbrella.[75] Their two virtues of being unmanned and preprogramed grant them advantages in testing opponents' anti-access area denial capabilities. Any combat attrition would be a matter of money and constructing more UCAVs and installing the artificial intelligence, and would not involve suffering the public fallout from service personnel fatalities and then the further process of training new aircrew. If a UCAV is shot down during "tense encounters", that might be a less escalatory scenario than the downing of a human piloted plane, yet a more likely outcome if no aircrew are involved in the operation.[76] This is a key question with autonomous systems as deterrence is under threat if decision makers are feeling emboldened by the perception that engaging in inherently destabilising military operations would not ultimately escalate beyond the threshold of armed conflict.

Escalation control

One of the major problems facing deterrence postures is that these technologies can be inflammatory and therefore attempting to prove deterrence by carrying out an equal or greater response to an incident might lead to serious instability through escalation. In the hypothesis section, this paper set out Clausewitz's observation of

[74] Kello, L. (2013), pp.7-40.
[75] Bronk, J. (2019), pp.99-104.
[76] Ibid, p.103.

the nature of war, to escalate once underway,[77] as being particularly relevant with the emergence of these new technologies which all have the capability to destabilise and escalate that instability into crises. Policy has to keep a tight rein over strategy and operations to maintain a clear focus on what sort of actions will and will not cause instability. This can be advertent or inadvertent if actors lose control and escalate beyond their intended strategic objectives.

Cyber offence excels when operating in the 'grey zone' between peace and armed conflict, and any attacks made then increase the likelihood of escalation by states operating with a deterrence posture. 'Active defence' in cyber conflict involves imposing a cost on an aggressor rather than 'passive defence' which is based upon hardening systems against penetration.[78] If a state with a deterrence posture chooses to enforce a cost upon the aggressor with an equal or greater response, then that imposition of cost will either deescalate and deter other adversaries from aggression if they perceive that cost to be too high to risk continuing cyber offence. This is a successful deterrence example but does rely on successful attribution of the cyberattack. The alternative is that an imposition of cost, in "the fog of cyber conflict, where who is actually doing what may be uncertain" might then "be seen by that adversary as an offensive act itself".[79] Cyber offence has this capability to provoke deterrence responses to escalate a dispute into a conflict or to give the initial aggressor a *casus belli* to escalate themselves. The role of the criminal sector also has unsettling implications for escalation control. If there is not enough oversight from the state on either policing the cyber offence criminal operators or supervision if they are being used by the state to further foreign policy through cyber offence, with

[77] Clausewitz, *On War*, tr. Howard and Paret, p.77.
[78] Lin, H. (2012), p.51.
[79] Ibid, pp.51-52.

plausible deniability being the key factor in their employment, then escalation might occur. An example of this are the attacks on Ukrainian state power grids at the end of 2015, attributed to Sandworm, a Russian hacking group, and the Ukrainian government blamed the Russian government for the cyberattacks, presumably suspecting their oversight on the attack.[80] Accidental escalation through human error outside a state's control in a cyber offence operation therefore can have unforeseen escalatory implications which evolve a conflict.[81]

The critical problem facing decision makers over LAWS when trying to pursue their state's strategic objectives is how do to achieve escalation control in situations where key decisions that have escalatory elements are taken by autonomous systems. Miller, a former Under Secretary for Defense, and Fontaine write that autonomous systems are "creating potential slippery slopes of escalation" and that "unless measures are taken to cushion the consequences of these military trends, conflict may become more probable and escalation more dramatic and severe".[82] Caitlin Talmadge refutes these claims and argues in her recent work that these emerging technologies are not sufficient independent drivers of escalation at this point in time. However, she concedes that they are in immature stages at this moment and could "generate inadvertent escalatory pressures" in the future. Her main argument is that "technology might enable escalation that states want to pursue anyway, and in fact states may pursue technology precisely for this reason".[83] This reasoning certainly backs up cyber offence as a tool for escalation, advertent or inadvertent, yet LAWS does require certain circumstances for escalation.

[80] Kostyuk, N., Powell, S., Skach, M. (2018), p.123.
[81] Lin, H. (2012), p.52.
[82] Miller, J.N., and Fontaine, R. (2017), p.36.
[83] Talmadge, C. (2019), p.866.

There are two scenarios where LAWS do have serious escalatory concerns which can trigger deterrence responses inadvertently. The first can be seen in the context of defensive LAWS, those currently enforcing missile/aerial defence for example such as the Phalanx and related CIWS systems which carry out lethal functions with autonomy. The Iron Dome and Pac-3 Patriot also integrate autonomy into targeting and firing decisions.[84] A judgement has to be made by the LAWS over what constitutes a threat. A human piloted plane armed with missiles flying at a military capability deployed with LAWS can be judged to be a threat, but what about ones flying at a different angle past it? If they are judged as threats by the LAWS and fired upon without having attacked first or openly aimed to attack, then that can be escalatory if it results in human casualties, seemingly an unprovoked attack. The second example is far more future leaning looking at LAWS in an offensive manner. Again, targeting errors, such as misidentifying combatants or military facilities in a first strike, might again escalate a situation beyond the strategic objectives of the state employing the LAWS. Both of these examples have consequences for deterrence as inadvertent mistakes by LAWS, which are carrying out escalatory decisions, mistakes which may not have been made by human operators, then are tests for the victim state's deterrence postures. LAWS in these examples have escalated disputes into crises, whereby escalation from the defender would be in line with their deterrence postures to then re-establish that deterrence.

Machine speed fighting, because of the speed of engagements, penalises self-defence military postures as they might be forced into change from a deterrence stance into an active defence posture, with weapons and capabilities on permanent high alert. Horowitz observes that "Countries could fear that an aggressor, using

[84] Horowitz, M.C. (2019), p.773.

LAWS or related systems operating at machine speed, could quickly knock out their command and control capabilities, eliminating their ability to retaliate".[85] If states are already at high alert then there are no more rungs on the escalation ladder to climb beyond armed conflict. To guarantee security, any posturing would have to be treated as an act of war because of the machine speed of the LAWS. A state could not afford to be trusting with such a threat to their own command and control. This brings the paper back to Talmadge's argument that technology might be pursued by states for the purpose of escalating rather than to deter.[86] Deterrence postures would be obsolete if LAWS reached a point where there is no opportunity for a state to respond in an equal or greater manner due to the initial first strike devastation, leaving no off ramps to deescalate.

HGVs might hamper escalation control at the highest levels of conventional warfare, where the mere presence, deployment or firing of an HGV might trigger a nuclear response. HGVs can test nuclear deterrence in how threatening they are perceived to be by states. The United States has stated that their HGVs will be conventional weapons, excluding them from the nuclear domain.[87] A potential issue is the risk of 'entanglement' where because HGVs are "dual use delivery systems that can be armed with nuclear and non-nuclear warheads" in China and Russia, which therefore involve "the commingling of nuclear and non-nuclear forces and their support structures".[88] This entanglement of nuclear and non-nuclear dual use HGVs increases issues in early warning systems and targeting. Due to the speed of the HGV, it would be extremely difficult for a nuclear armed state to judge whether the

[85] Ibid, p.782.
[86] Talmadge, C. (2019), p.866.
[87] United States, U.S. Department of Defense, "Department of Defense Tests Hypersonic Glide Body", (2020). www.defense.gov/Newsroom/Releases/Release/Article/2119458/department-of-defense-tests-hypersonic-glide-body/
[88] Arbatov, A., Dvorikin, V., Topychkanov, P., Zhao, T. and Bin, L. (2017).

warhead is nuclear in the short flight time. There is the potential then for that state to escalate to a nuclear response if it feels sufficiently threatened by the HGV. Nuclear deterrence would therefore be tested by even a conventional HGV launch.

Deterrence postures therefore are becoming more difficult to uphold with not just the proliferation of technologies incentivising offence and first moves but also the nature of deterrence postures. They can invite escalation to reach a point where to re-establish deterrence the defender must use force to cow the aggressor into deescalating. Decision makers will face hard choices whether to give teeth to their own deterrence postures, risking escalation beyond a point of no return, or to be a victim of 'death by a thousand cuts', whereby deterrence postures are whittled down to little value and the lack of action enables the erosion of a state's power.

Trust and signalling problems

A significant issue in attempting to deter serious cyberattacks is the problem of signalling. Lin argues that "communicating to an adversary the nature of any such thresholds regarding activity in cyberspace may be particularly problematic, even under normal peacetime circumstances".[89] This can lead to inadvertent escalation through either counter operations, cyber or military, or other forms of imposing cost on the actual aggressor or those perceived of wrongdoing, in both ways escalating the situation. The lack of clarity in the fog of cyberspace therefore is harder to signal a clear cyber deterrence posture, particularly when state critical infrastructure is reliant on private companies such as financial institutions. A cyber offensive operation might target a private actor which then forces the state to either step in and expend geopolitical capital. Or a state might choose to ignore it and incentivise further attacks as a deterrence red line has either been overstepped or it was never

[89] Lin, H. (2012), p.52.

imposed to begin with. Jon Lindsay argues that states make a conscious effort to not impose costs on aggressors for low-level cyberattacks, arguing that "toleration for low-level aggression is the price of credible deterrence against serious attacks".[90] This viewpoint would therefore indicate that sub threshold deterrence against cyber offence is either not possible due to the volume of attacks or the attacks themselves are low-level enough to have not imposed a cost significant enough to warrant an equal or greater response, or indeed it could be a combination of the two. Signalling therefore suffers as if states only respond to the larger cyberattacks, then relying on the judgement of the cyber attacker to define where the line is themself is a riskier strategy. Those red lines are then up for debate and could have escalatory consequences.

Trust in one's own capabilities and the ability to signal credibility to any potential aggressors is a key component of deterrence. LAWS are particularly troublesome for states employing them in both of these aspects. LAWS are extremely new technology, which are constantly being upgraded and acquiring battlefield roles, with the prediction that they will be used in offensive operations in the future.[91] Therefore establishing trust in a LAWS will require extensive testing, more than other systems as relying on autonomy over human controlled systems is a risk which commanders are less inclined to take. Extensive testing is needed in trying to dispel automation bias and also therefore rid command and control of any pre-existing tendencies to trust manned systems more.[92] The arms race of LAWS at this point, in states' drive to operate at machine speed fighting, might lead to less testing to roll out operational LAWS earlier than militaries would do for other systems. This lack of testing and

[90] Lindsay, J. (2015), p.54.
[91] Work, B. (2015).
[92] Horowitz, M. (2019), p.774.

therefore faith in LAWS prematurely installed in a state's arsenal might weaken their deterrence postures if they rely on systems which might not fulfil their intended task of deterring an enemy by failing to effectively punish any transgressors.

The second aspect is the difficulty for a state to signal to an adversary that their LAWS are credible and that any transgression would have overwhelmingly negative consequences for the offender. Uncertainty can be generated because autonomous systems rely on code which cannot be shared with the enemy. Without sharing the programming with any rivals, it is much harder to signal credibility over what LAWS are programmed to do in certain situations, such as boundary transgression or anti access area denial capabilities. If lethal functions have been delegated outside of the command and control structures to LAWS, and the state deploying the LAWS is unwilling to share programming, then there should be great uncertainty over attempting to predict a hostile state's behaviour. If the hostile state does not believe that the LAWS opposed against them is a credible enough to deter them, then that invites an attack thus weakening the deterrence posture as a whole.[93] The lack of control the LAWS state has ceded in return for operational speed therefore has the ability to escalate inadvertently.

HGVs have issues with trust and signalling as well despite being operated by states with no-first-use policies, and possessing only conventional warheads in the case of the United States. Their capabilities point towards effective first strikes in knocking out command and control structures as well as targeted strikes against physical offensive assets like carriers, or forward operating bases. Whether they are used first is not really the operative factor, but instead it is the perception in capabilities of the weapons in the hands of rival powers which is more consequential for deterrence

[93] Ibid, p.765.

postures. The speed of delivery already makes states which employ them have threatening, high alert postures. Two HGV armed states are capable of decimating each other's major population centres in minutes, whether tensions between them are healthy or not.[94] An HGV bolstered deterrence posture, perceived to be high-readiness by others due to the speed of delivery, can be seen in two manners. It might be regarded as a strong deterrent in that states would not want to risk escalating a HGV armed state. Alternatively, it could hold more risk because HGV speeds indicate that first strikes might be the only way to ward off an HGV armed state. Any period of instability or crisis might then warrant the response of knocking out their command and control of an HGV armed state, thereby weakening the effect of deterrence.

Deniability

The attribution problem is applicable to both cyber domains and LAWS. A hypersonic glide vehicle which causes fatalities would be reasonable to blame on only Russia, China or the United States, which currently have those capabilities and will be the only ones likely to have them for the next ten years.[95]

"Doing attribution well is at the core of virtually all forms of coercion and deterrence, international and domestic. Doing it poorly undermines a state's credibility, its effectiveness, and ultimately its liberty and its security".[96] Cyber attribution is not a binary, solvable or unsolvable problem according to Rid and Buchanan. It is instead an art, a multi layered nuanced process, which involves matching resources for

[94] Acton, J. (2014), 'The Arms Race Goes Hypersonic', *ForeignPolicy.com*. foreignpolicy.com/2014/01/30/the-arms-race-goes-hypersonic/
[95] Chuter, A. (2019), 'British military scrambles to speed up work on hypersonic engines, weapons', *DefenseNews.com*. www.defensenews.com/global/europe/2019/07/18/british-military-scrambles-to-speed-up-work-on-hypersonic-engines-weapons/
[96] Rid, T. and Buchanan, B. (2015), p.4.

attribution to the severity of the consequences of a cyber incursion.[97] Rid and Buchanan therefore argue that deterrence of high-impact cyber offence is achievable as states, larger ones with the resources and time, increase foreign trust in the system of attribution when they decide to act on punishing a cyber offender.[98] Deterrence by punishment is consequently tenable under the correct circumstances. Conversely, deterrence at lower levels must be harder, particularly sub threshold actions which are not particularly financial harmful or devastating to a state's security, as investing resources to attribute all cyberattacks at any level would be impossible. Whether or not attribution is correctly done well, a state may simply choose to deny the attack, or indeed outsource cyber offence to the private or criminal sectors to provide a deniable buffer between the state and the cyberattack.[99] The cyberattacks on Estonia in 2007 proved Rid and Buchanan's argument that resources and time are required to attribute cyberattacks successfully, something almost exclusively limited to larger states with greater funding. Senior Estonian officials were quick to blame Russia yet they were not able to gather sufficient evidence for a successful attribution. Russia responded with by denying the cyberattacks, thereby proving to other potential cyber aggressors that Estonian attribution skills were poor, weakening future attempts to deter cyber offence.[100] Deterrence then in a cyber field might only be limited to the largest states attempting to deter the higher impact attacks, and so in other cases deniability allows further transgression.

There is a case for plausible deniability in how LAWS can weaken deterrent postures. This is ultimately down to the lack of accountability which LAWS have

[97] Ibid, p.7.
[98] Ibid, p.31.
[99] Farwell, J.P. and Rohozinski, R. (2011), p.24.
[100] Rid, T. (2012), p.12.

when carrying out lethal functions without human supervision. A state can plausibly deny that it ordered an attack if there was no human in the decision-making chain. It can point to the idea that if the programming was correct, then the victim state must have transgressed or identified itself as a threat to justify the lethal function which followed. Any attempt to pin down the accountability of the lethal function to a single commander or programmer or even the machine itself would be not be satisfactory.[101] State governments can deny and then deescalate a situation away from armed conflict, which this paper predicts will become a normalised occurrence in areas where anti access area denial autonomous weapons are positioned. This makes it harder to deter these disputes and conflicts as blame is impossible to prove in international law currently for LAWS if no commander or decision maker actually gave an order to execute lethal measures.[102]

With the advancement of these new technologies, a state can therefore be worried about the effectiveness of a deterrence posture through the proliferation and the engagement with these new means of achieving strategic objectives. There should be deep concern that any rival power armed with them would utilise them in a hostile manner. With deterrence defanged, instability and conflict become cases of when, not if, for global powers.

Chapter 4: Concluding thoughts: state stability and future policy

State stability

[101] Sparrow, R. (2007).
[102] Crootof, R. (2016).

Robert Powell argued that to ensure stability between states, there are four conditions to be met:

1) There is no risk of a purely accidental attack.
2) That if a state has the option of attacking, it also has the option of submitting to its adversary.
3) That no state will attack unless it believes that the probability that war is inevitable is greater than fifty percent.
4) That the first three conditions are known and accepted as valid by all potential belligerents.[103]

By identifying the conditions to ensure stability, one can also see the potential sources of instability, which are exacerbated by the proliferation of these new technologies.

Powell's first condition is at risk then with the outsourcing of lethal functions to LAWS, that an attack can be undertaken without a decision maker giving the order. Cyberattacks themselves may originate from the criminal sector or non-state actors operating within a state, advertently or inadvertently fulfilling that state's foreign policy objectives. Both of these examples have destabilising results in relations between powers as there is scope for a break down in trust between those states and the potential for escalatory retaliation.

Powell's second condition is threatened by the development of both LAWS and HGVs. As early as 2007, the stated goal of advancements in LAWS is to achieve an operational speed of 'machine speed' thinking and fighting, outmatching human operators.[104] Haas and Fischer argue that LAWS' ability to knock out command and

[103] Powell, R, (1989), p.70.
[104] United States, U.S. Department of Defense, 'Unmanned Systems Roadmap 2007-2032', (2007). apps.dtic.mil/dtic/tr/fulltext/u2/a475002.pdf.

control centres and to decimate opposition leadership swiftly will create serious instability in lowering the threshold for conflict initiation. They propose that LAWS will offer a “significant, set of advantages to actors engaging in targeted killings” and “an expansion of targeted killings as a result of the availability of autonomous aerial weapons could significantly lower the threshold for the initiation and pursuit of long-lasting gray zone conflicts, with the potential for escalation from sub-conventional into large-scale conventional wars”.[105] LAWS therefore might not offer the ability for a state to submit before an attack becomes overwhelming or existential to its survival, creating instability and first strike imperatives. Likewise, HGVs stated capability in defeating any current missile defence through their speed and manoeuvrability might also have the ability to target leadership, population centres and command structures, which also has the same implications for stability.

Powell’s third condition is tied to the concept that war between a status quo power and revisionist power is inevitable, brought upon by a hegemon’s fear of being surpassed. Thucydides used the example of “the growth of the Athenians to greatness” which “brought fear to the Lacedaemonians and forced them to war”.[106] Any state which sees rivals proliferate these technologies then, and judges them to be threats to their deterrence postures because of the incentives of attacking provided by the offence-dominance, might then feel that the prospect of conflict is above fifty percent and prepare for that conflict. They might even initiate it to gain that first move advantage, a prospect inherently dangerous to international stability.

Perception of threat, capabilities and intentions finally governs the final condition of a universal understanding by all states engaging with these new technologies. If a state knows about the risks of LAWS and HGVs to their own command and control

[105] Haas, M. and Fischer, S. (2017), pp.299-300.
[106] Thucydides, *History of the Peloponnesian War*, tr. Smith, C.F. 1.23.

functions, and another state also proliferating the same technologies has a separate view on their abilities, then that mismatch might provoke instability. This is because the former state's threshold for escalation could be lowered in comparison to the latter. Any arms build-up by the latter state might then also be interpreted by the former state in the security dilemma which follows as far more threatening than what the latter state intended. This then encourages a further build up by the former or a first move.

An alternative view on stability, put forward by Aaron Miles, is that there are two types of strategic stability which states can aspire to: neutral stability and true stability.[107] Neutral stability has been the typical focus for states like the United States, a focus on removing instability rather than providing stability.[108] Neutral stability favours strong states with superior conventional military capabilities. This type of foreign policy, which Miles argues the United States have been pursuing, leans towards an arms race build up to attempt to establish a form of deterrence and limit crisis instability. New technologies here would be part of a survivable second-strike arsenal, with cyber offence being the only out of the three to be used in any form of a first strike. The 'true stability' prospect is one which Miles claims to favour states with inferior capabilities and revisionist aims. This is important when looking at Russia and China, which might follow a strategy of escalating to deescalate, looking at a devastating *fait accompli*. This would be accompanied by stabilising systemic forces to then deescalate the crisis, a prospect most likely also backed by the state on the receiving end of any threatened or actual escalation.[109] A devastating first strike to achieve true strategic stability would then be greatly incentivised by

[107] Miles, A. (2016), pp.426-428.
[108] Ibid, p.423.
[109] Ibid, p.428.

operationalised LAWS and HGVs if they feel that deterrence is impotent enough to get away with that sort of escalation. State stability therefore might be strengthened in the long term through the proliferation of these technologies, if states choose to pursue 'true stability' by reshaping the international order to their liking.

Future policy

As a result of these emergent technologies' effects on deterrence, deterrence postures, and the threat they therefore pose to state stability, what policies should major powers pursue in an attempt to re-establish deterrence and affirm their commitments to strategic stability?

For states wanting to pursue a deterrence posture, sub threshold elements, particularly within cyber offence or individual disputes over LAWS, like an unintended lethal exchange, then any attempt to retaliate to re-establish deterrence might have to involve an equal or lesser response, and not necessarily linked to military action. An example of this in action is the United Kingdom's response the poisoning of the Skripal family in 2018, expelling 23 Russian diplomats and gathering a consensus amongst 28 other states to expel a total of 153 Russian diplomats, which may have significantly weakened Russian HUMINT operations within those states.[110] Significantly, the UK exercised deterrence by punishment without engaging in a similar exchange of an assassination attempt on Russian soil, but instead enacted a non-lethal response to re-establish deterrence while not escalating to a lethal exchange. This can be a model, particularly for deterring cyber offence operations, to still attempt to maintain international state stability, whereby imposing costs without escalating is possible as response to inflammatory attacks.

[110] Dewan, A. and Gigova, R. (2018), 'Russian Diplomats Expelled from UK Head Back to Moscow', *CNN*. edition.cnn.com/2018/03/20/europe/russia-diplomats-leave-uk-intl/index.html

Garfinkel and Dafoe's article on how the offence-defence balance scales points to heavy investment as being an important factor in swinging the balance back towards defence.[111] Investing in more defence capabilities including the innovation as well as breadth of defence coverage is a policy option therefore, although to fund this would require vast political capital and willpower. If HGVs are do create a missile offence which current or envisioned future defence might not be able to deter, with the ability to take out fixed runways on land, then perhaps aircraft carriers which can be moving might then be a platform to exercise operationalised power and deter HGV strikes through their survivable second-strike factor. If aircraft carriers are also too vulnerable to HGV capabilities, or the machine speed fighting capability of offensive LAWS, then investing in attack submarines with advanced stealth technology might deter first strikes by maintaining a state's second-strike ability.

Establishing norms over the usage of LAWS now through their immediate use and demonstrations might create a favourable climate of consensus amongst major powers in terms of non-proliferation of the technology. To promote an arms control norm, there must be buy in from those states actually investing in the technology, which will not be brought about while states view LAWS in the context of their battlefield advantage at the expense of their strategic stability. A demonstration of their use in a battlefield context at their most potent might bring about concerted global arms control initiatives.

[111] Garfinkel, B. and Dafoe, A. (2019).

Bibliography

Books

Carl von Clausewitz. (1989). *On War*, translated by Michael Howard and Peter Paret, Princeton University Press.

Citino, Robert M. (2005). *The German Way of War: From the Thirty Years' War to the Third Reich*. University of Kansas Press.

Liddell Hart, Basil H. (1960). *Deterrence or Defence*. Stevens and Sons.

Lieber, Keir A., and Press, Daryl G. (2020). *The Myth of the Nuclear Revolution: Power Politics in the Atomic Age*. Cornell University Press.

Mearsheimer, John. (2001). *The Tragedy of Great Power Politics*. W.W. Norton & Company.

Sofaer, Abraham David, and Goodman, Seymour E. (2001). *The Transnational Dimension of Cybercrime and Terrorism.* Hoover Institution Press.

Thucydides. (1919). *History of the Peloponnesian War, Volume I: Books 1-2*, translated by C. F. Smith, Harvard University Press.

Waltz, Kenneth N. (1979). *Theory of International Politics*. Waveland Press.

Publications

Japan Ministry of Defence, *Outline of the National Security Strategy*, 2015.

Ministry of Foreign Affairs of the People's Republic of China, *Position Paper of the People's Republic of China at the 66th Session of the united Nations General Assembly*, 2011.

State Council, *China's National Defense in the New Era*, 2019.

U.S. Department of Defense, *Unmanned Systems Roadmap 2007-2032*, 2007.

United Kingdom, Ministry of Defence, *National Security Strategy and Strategic Defence Review 2015*, 2015.

U.S. Department of Defense, *Department of Defense Announces Successful Micro-Drone Demonstration*, 2017.

U.S. Department of Defense, *Media Availability With Deputy Secretary Shanahan and Under Secretary of Defense Griffin at NDIA Hypersonics Senior Executive Series*, 2018.

U.S. Department of Defense, *Nuclear Posture Review 2018*, 2018.

U.S. Department of Defense, *2019 Missile Defense Review*, 2019.

U.S. Department of Defense, *Department of Defense Tests Hypersonic Glide Body*, 2020.

The White House, *National Security Strategy of the United States of America,* 2017.

Papers

Altmann, Jürgen., and Sauer, Frank. (2017). Autonomous Weapon Systems and Strategic Stability, *Survival*, 59:5, 117-142.

Arbatov, Alexey., Dvorkin, Vladimir., Topychkanov, Petr., Zhao, Tong., and Bin, Li., (2017). Entanglement: Chinese and Russian Perspectives on Non-nuclear Weapons and Nuclear Risks, *Carnegie Endowment for International Peace*.

Bronk, Justin. (2019). The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk, *Stockholm Internattional Peace Research Institute*, Volume I Euro Atlantic Perspectives, 99-104.

Center for Security Policy, & VanNess, A. (2013). Israeli Innovators in National Security Technology: Case Studies for US and International Technology Transfer, *Center for Security Policy*, 24-27.

Clarke, Rachel, M.D., and Youngstein, Taryn, M.D. (2017). Cyberattack on Britain's National Health Service — A Wake-up Call for Modern Medicine, *The New England Journal of Medicine*, 377, 409-411.

Crootof, Rebecca. (2016). War torts: Accountability for autonomous weapons, *University of Pennsylvania Law Review,* 164:6, 1347-1402.

Edwards, Benjamin., Furnas, Alexander., Forrest, Stephanie., & Axelrod, Robert. (2017). Strategic aspects of cyberattack, attribution, and blame, *Proceedings of the National Academy of Sciences of the United States of America*, 114:11, 2825-2830.

Farwell, James P., and Rohozinski, Rafal. (2011). Stuxnet and the Future of Cyber War, *Survival*, 53:1, 23-40.

Garcia, Denise. (2018). Lethal Artifiical Intelligence and Change: the Future of International Peace and Security, *International Studies Review*, 20:2, 334-341.

Ghafur, S., Kristensen, S., Honeyford, K. et al. (2019). A retrospective impact analysis of the WannaCry cyberattack on the NHS, *npj Digital Medicine*, 2:98.

Glaser, Charles L., and Kaufmann, Chaim. (1998). What Is the Offense-Defense Balance and How Can We Measure It?, *International Security*, 22:4, 44–82

Haas, Michael Carl., and Fischer, Sophie-Charlotte. (2017). The evolution of targeted killing practices: Autonomous weapons, future conflict, and the international order, *Contemporary Security Policy*, 38:2, 281-306.

Horowitz, Michael C. (2019). When speed kills: Lethal autonomous weapon systems, deterrence and stability, *Journal of Strategic Studies*, 42:6, 764-788.

Kello, Lucas. (2013). The Meaning of the Cyber Revolution: Perils to

Theory and Statecraft, *International Security,* 38:2, 7–40.

Kostyuk, Nadiya., Powell, Scott., & Skach, Matt. (2018). Determinants of the Cyber Escalation Ladder, *The Cyber Defense Review*, 3:1, 123-134

Lieber, Keir A., and Press, Daryl G. (2006). The End of MAD? The Nuclear Dimension of U.S. Primacy, *International Security*, 30:4, 7-44.

Lin, Herbert. (2012). Escalation Dynamics and Conflict Termination in Cyberspace, *Strategic Studies Quarterly*, 6:3, 46-70.

Lindsay, Jon R. (2015). Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyberattack, *Journal of Cybersecurity*, 1:1, 53-67.

Locatelli, Andrea. (2013). The Offense/Defense Balance in Cyberspace. *Istituto Per Gli Studi Politica Internazionale*, 203.

Lynn, William J. (2010). Defending a New Domain: The Pentagon's Cyberstrategy. *Foreign Affairs*, 89:5.

Maigre, Merle. (2015). 'Nothing New in Hybrid Warfare: The Estonian Experience and Recommendations for NATO'*. German Marshall Fund of the United States*.

Miles, Aaron. (2016). The Dynamics of Strategic Stability and Instability, *Contemporary Security Policy*, 35:5, 423–437.

Miller, James N., and Fontaine, Richard. (2017). A New Era in U.S.-Russian Strategic Stability, *Center for a New American Security*.

Oelrich, Ivan. (2020). Cool your jets: Some perspective on the hyping of hypersonic weapons, *Bulletin of the Atomic Scientists*, 76:1, 37-45.

Pan, Zhengiang. (2018). A Study of China's No-First-Use Policy on Nuclear Weapons, *Journal for Peace and Nuclear Disarmament*, 1:1, 115-136.

Powell, Robert. (1989). Crisis Stability in the Nuclear Age, *The American Political Science Review*, 83:1, 61-76.

Pynnöniemi, Katri. (2018). Russia's National Security Strategy: Analysis of Conceptual Evolution, *The Journal of Slavic Military Studies*, 31:2, 240-256.

Rid, Thomas. (2012). Cyber War Will Not Take Place, *Journal of Strategic Studies*, 35:1, 5-32.

Rid, Thomas., and Buchanan, Ben. (2015). Attributing Cyber Attacks, *Journal of Strategic Studies*, 38:1-2, 4-37.

Roff, Heather M. (2014). The Strategic Robot Problem: Lethal Autonomous Weapons in War, *Journal of Military Ethics*, 13:3, 211-227.

Rydell, Randy. (2020). The Guterres Disarmament Agenda and the Challenge of Constructing a Global Regime for Weapons, *Journal for Peace and Nuclear Disarmament*, 3:1, 21-40.

Saltzmann, Ilai. (2013). Cyber Posturing and the Offense-Defense Balance, *Contemporary Security Policy*, 34:1, 40-63.

Schneider, Jacquelyn. (2019). The capability/vulnerability paradox and military revolutions: Implications for computing, cyber, and the onset of war, *Journal of Strategic Studies*, 42:6, 841-863.

Sheng, Li. (2013). When Does Internet Denial Trigger the Right of Armed Self-Defense?, *Yale Journal of International Law*, 38:1, 179-216.

Slayton, Rebecca. (2017). What Is The Cyber Offense-Defense Balance?: Conceptions, Causes and Assessments, *International Security*, 41:3, 72-109.

Sparrow, Robert. (2007). Killer Robots. *Journal of Applied Philosophy*, 24:1, 62-77.

Talmadge, Caitlin. (2019). Emerging technology and intra-war escalation risks: Evidence from the Cold War, implications for today, *Journal of Strategic Studies*, 42:6, 864-887.

Tannenwald, Nina. (1999). The Nuclear Taboo: The United States and the Normative Basis of Nuclear Non-Use. *International Organization*, 53:3, 433-468.

Tariq, Nida. (2018). 'IMPACT OF CYBERATTACKS ON FINANCIAL

INSTITUTIONS' *Journal of Internet Banking and Commerce*, 23:2.

Websites

Acton, James M. (2014). The Arms Race Goes Hypersonic. *Foreign Policy*. Accessed July 2 2020. foreignpolicy.com/2014/01/30/the-arms-race-goes-hypersonic/.

BBC News, (2018). Singapore personal data hack hits 1.5m, health authority says, *BBC News*. Accessed August 1 2020. www.bbc.co.uk/news/world-asia-44900507.

Biswas, Soutik. (2020). India-China clash: 20 Indian troops killed in Ladakh fighting, *BBC News*. Accessed August 28 2020. www.bbc.co.uk/news/world-asia-53061476.

Chuter, Andrew. (2019). British military scrambles to speed up work on hypersonic engines, weapons, *DefenseNews*. Accessed July 29 2020. www.defensenews.com/global/europe/2019/07/18/british-military-scrambles-to-speed-up-work-on-hypersonic-engines-weapons/.

Congressional Research Service, (2020). Conventional Prompt Global Strike and Long Range Ballistic Missiles: Background and Issues, *Federation of American Scientists*. Accessed July 21 2020. fas.org/sgp/crs/nuke/R41464.pdf.

Dewan, Angela., and Gigovva, Radina. (2018). Russian diplomats expelled from UK head back to Moscow, *CNN*. Accessed August 4 2020. https://edition.cnn.com/2018/03/20/europe/russia-diplomats-leave-uk-intl/index.html.

Elgin, Ben. and Riley, Michael. (2014). "Now at the Sands Casino: An Iranian Hacker in Every Server", *Bloomberg*. Accessed June 2 2020. www.bloomberg.com/news/articles/2014-12-11/iranian-hackers-hit-sheldon-adelsons-sands-casino-in-las-vegas.

Field, Matthew. (2018). WannaCry cyber attack cost the NHS £92m as 19,000 appointments cancelled, *The Telegraph*. Accessed July 7 2020. www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled/.

Gady, Franz-Stefan. (2016), China Tests New Weapon Capable of Breaching US Missile Defense Systems, *The Diplomat*. Accessed June 21 2020. thediplomat.com/2016/04/china-tests-new-weapon-capable-of-breaching-u-s-missile-defense-systems/.

Garfinkel, Ben., and Dafoe, Allan. (2019). How does the offense-defense balance scale?, *Journal of Strategic Studies*, 42:6, 736-763.

Gorman, Siobhan and Barnes, Julian E. (2012), Iran Blamed for Cyber Attacks, *The Wall Street Journal*. Accessed May 29 2020. www.wsj.com/articles/SB10000872396390444657804578052931555576700.

Hersh, Seymour M. (2010). The Online Threat: Should We Be Worried about Cyber War?, *The New Yorker*. Accessed August 6 2020. www.newyorker.com/magazine/2010/11/01/the-online-threat.

Karako, Thomas., and Williams, Ian. (2017). Missile Defense 2020, *CSIS*. Accessed June 19 2020. missilethreat.csis.org/wp-content/uploads/2017/04/170406_Karako_MissileDefense2020_Web.pdf.

Langner, Ralph. (2013). Stuxnet's Secret Twin, *Foreign Policy*. Accessed June 29 2020. www.foreignpolicy.com/articles/2013/11/19/stuxnets_secret_twin_iran_nukes_cyber_attack.

Missile Threat. (2020). Avangard, *CSIS*. Accessed August 2 2020. missilethreat.csis.org/missile/avangard/.

Nakashima, Ellen., and Warrick, Joby. (2012). Stuxnet was work of U.S. and Israeli experts, officials say, *The Washington Post*. Accessed July 4 2020. www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html.

NATO, (2019). NATO will defend itself, *NATO*. Accessed April 29 2020. www.nato.int/cps/en/natohq/news_168435.htm.

Reif, Kingston., and Bugos, Shannon., (2020). Pentagon Tests Hypersonic Glide Body, *Arms Control Association*. Accessed August 20 2020. www.armscontrol.org/act/2020-04/news/pentagon-tests-hypersonic-glide-body.

Slater, Joanna., and Constable, Pamela. (2019). Pakistan captures Indian pilot after shooting down aircraft, escalating hostilities, *Washington Post*. Accessed August 11 2020. www.washingtonpost.com/world/asia_pacific/pakistan-says-it-has-shot-down-two-indian-jets-in-its-airspace/2019/02/27/054461a2-3a5b-11e9-a2cd-307b06d0257b_story.html.

Stowe-Thurston, Abigail., Korda, Matt., and Kristensen, Hans M. (2018). Putin Deepens Confusion About Russian Nuclear Policy, *Russia Matters*. Accessed August 24 2020. www.russiamatters.org/analysis/putin-deepens-confusion-about-russian-nuclear-policy

U.S. Navy, (2019). MK 15 – Phalanx Close-In Weapon System (CIWS. Accessed August 10 2020. www.navy.mil/Resources/Fact-Files/Display-FactFiles/Article/2167831/mk-15-phalanx-close-in-weapon-system-ciws/.

Work, Bob. (2015). The Third U.S. Offset Strategy and Its Implications for Partners and Allies, *U.S. Department of Defense*. Accessed May 22 2020. www.defense.gov/Newsroom/Speeches/Speech/Article/606641/the-third-us-offset-strategy-and-its-implications-for-partners-and-allies/.