

Is “Nuclear Deterrence” still a relevant strategy for the 21st Century?

James Morgan




Journal of International Affairs & Politics

Vol. 10

**Is “Nuclear Deterrence” still
a relevant strategy for the
21st Century?**

by James Morgan

July 2017

© Copyright 2017  IRIA
International Relations Insights & Analysis
All rights reserved.

For more information about IRIA visit:
www.ir-ia.com



INTERNATIONAL RELATIONS INSIGHTS & ANALYSIS

International Relations Insights & Analysis (IRIA) is a research institute focusing on critical issues that threaten international peace & security. IRIA investigates and offers research and analysis on security, energy, terrorism, foreign affairs as well as global political agendas. We formulate independent, concise and meaningful research presented in an informative and interactive manner.

IRIA special reports include experts' opinion, special features, cost & benefit analysis. IRIA also examines risk & opportunities, highlight common threats and misconceptions and provide improved set of strategies and countermeasures. The key findings of reports and analysis highlight pragmatic policy options and revise strategies.

IRIA aims to support grassroots democracy, promote peace building processes and cultural harmony by working with scholars, policymakers and institutions.

Introduction

The problem with the current nuclear deterrence is that the attitude surrounding its basic ideology is still based on a post-war era of inflated egos between entire nations, taking only into account who has the biggest and best. Technology and political landscapes have changed to a point where theories and practices from nearly half a decade ago, are no longer as poignant as they should be. Deterrence comes hand in hand with non-proliferation, they are needed to check each other, to prevent either a return to the days of hyper-proliferation, or to prevent an uneven and opportunistically volatile one-sided disarmament process. The 21st Century has seen the development of contested and troublesome behavior. Iran and North Korea's quests for nuclear capability, US protection of Israel's desire to maintain their offensive rhetoric surrounding Iran as well as UK and US apparent decrease in hardware whilst adamantly renewing and upgrading their weapons systems, are all examples of problems facing the global community in the 21st Century.

The only trouble being, this generation of deterrence theory has the added complications of hybrid warfare, meaning no longer can states instantly identify their attackers. Moreover, their attackers are not the uniformed armies of another nation, they are terror cells, state-sponsored terrorism, lone wolf attackers, cyber attackers and non-uniformed military groups. Developments in cyber warfare as well as the ever-expanding market for private military and security contractors are two examples of the complexity of modern hybrid warfare which cannot be allowed to be compatible with a traditional deterrence theory. This essay will focus on why with the rise of uncertainty-promoting hybrid warfare, nuclear deterrence

against conventional nation-nation attacks as well as a deterrent against other aggressive or undesirable actions in general, are both flawed. Mistakes happen, manipulations of computer systems are all too easy and tempers are fraying in volatile parts of the globe. Nuclear deterrence is best pictured as a carefully constructed house of cards, next to an open window. It exists in its originally constructed form, however now the wind has changed, we do not know for how long, and yet nobody appears willing to begin the disassembly or appropriate reconfiguration. Is it wise to take a "if it's not broke, don't fix it" approach? This essay will discuss how a traditional deterrence theory approach is no longer compatible with the 21st century security threats.

The Co-Dependent Relationship between Deterrence Theory and Non-Proliferation

Nuclear deterrence and the Non-Proliferation Treaty (NPT), along with other treaties and less formal agreements, are at this moment in time reliant in propping each other up and create a duality within the discussion, but are incompatible with the dynamism and unpredictable anonymity of today's world. After-all why would a nuclear weapon state (NWS) agree to make any drastic reductions in their nuclear status and risk a shift in a delicate nuclear world-order, which is founded upon deterrence theory?

The traditional deterrence theory relies upon three main preconditions that are necessary for successfully utilising a deterrent. The first precondition is communication - the very nature of a deterrent is to prevent a party from carrying out an act that is undesirable to oneself. For this to be achievable at the most basic, child's play-ground level, the coercive party must make clear what the exact action



A missile is carried by a military vehicle during a parade to commemorate the 60th anniversary of the signing of a truce in the 1950-1953 Korean War, at Kim Il-sung Square in Pyongyang on July 27, 2013. Photo Credit: REUTERS/Jason Lee.

is, which is unacceptable. I am reminded of the importance of a social aspect in regards to this precondition by the typical school child's threat of "if you do that, I'll tell on you", this aspect does not change at the international or transnational level. The second precondition is that of capability - no threat can be seen as legitimate if there is no belief the coercer is actually willing to go through with the retributive action. Lastly the action being used as a coercive deterrent must be credible - the party being threatened will assuredly receive greater damage than the coercive party, and thus the end result is acceptable only to the coercer and not the coerced due to "unacceptable losses". During the Cold War, the enormous nuclear stockpiles of both the US and the Soviet Union made the threat of nuclear war a capability, the threat was also credible as in the face of potentially mutual assured destruction (MAD), neither party had anything to lose. The case of credibility was also strengthened on the part of the US, as they had precedent as the only country to this day to deploy nuclear weapons in times of war against their enemy. These three preconditions form the basis of traditional deterrence theory

still employed to this day, despite the drastic changes and advancements of the world stage. Structurally inherent to deterrence and a characteristic which separates it from coercive compellence, is that it requires no time limit. While this may appear a positive attribute in that the opportunity for stability or peace is also perpetual, in reality all this means is that while the deterrent theory may not change, the risks and contributing socio-historic-economic factors, do.

I believe, when considering the 21st Century deterrence, it's also important to consider the practicalities surrounding the non-proliferation regime. The Non-Proliferation Treaty (NPT) is undoubtedly the cornerstone of the de-escalation and associated taboos surrounding NW use after the cold war. The regime also incorporates the Partial Test Ban Treaty, the Comprehensive Test Ban Treaty, the Fissile Material Cut-off Treaty, the Strategic Arms Limitation Talks (SALT) 1 and 2, as well as a whole myriad of other bilateral agreements and treaties (Sidhu, 2013; Byrne, 1988). What these arrangements and limitations have done, is support and foster the deterrence theory

that grew out of the cold war. The NPT aims to keep a cap on the quantitative capabilities as to prevent another self-perpetuating arms race that would escalate the requirements for the "capability" precondition among nations. The various "non-testing/developing" treaties aim to ensure the current NWS remain as such, whilst maintaining their technological dominance and thus reinforcing their "credibility" within the deterrence theory. Lastly the various informal talks, bilateral agreements and negotiations such as SALT, aim to keep open this avenue of communication, the first precondition for deterrence. The duality of this scenario however is while it maintains this fragile non-use taboo among nations, it seems almost redundant.

The non-proliferation regime is necessary to underpin deterrence theory, which in turn gives a rationale for furthering and strengthening the regime. Now while this may continue indefinitely, with no major alterations to the status quo of the international community, if we no longer see frequent conventional warfare between nation-states, but rather a new threat emerging from alternative and hybrid warfare, what use are the enormous stockpiles of continually re-developed nuclear weapons, against smaller groups and unidentifiable enemies. A nuclear weapon is not an effective deterrence towards a terror network such as ISIL due to the rules of proportionate warfare, common sense and normative taboos, which prevent their use. A large nuclear weapon arsenal is likewise no real deterrence towards the cyber-attacks of any nation, because firstly they can be denied and secondly, such attacks are not currently sufficient evidence of an act of war to legitimise a nuclear response. Is it possible the symbiotic relationship between the non-proliferation regime and traditional deterrence theory have reached their cooperative limit and will now

begin to stagnate, with the risk of volatility and probability of accidents increasing over time.

This essay will not include a detailed alternative to this situation as that topic alone would require its own analysis of nuclear disarmament, but to give a rounded appreciation of the scenario described herein, an alternative in the mind of the writer would appear something similar to the "weaponless deterrent" as put forward by Nick Ritchie . As many countries have claimed to have hit an 'irreducible minimum' in their nuclear stockpiles (Ritchie, 2014: 607), combined with the stagnating and outdated scenario of deterrence explained here, this appears to be the best hypothesized vision of the minimal role left for NW technology to be resigned to.

21st Century Changes – Cyberwarfare, Intelligence and Private Military Contractors

The most obvious advancement in 21st century technology is the ability to manipulate information technology. The terminology and nomenclature is still loosely used and unconfirmed, with many questions recently raised as to what qualifies as an act of cyberwar (normally between nations, equivalent to that of a conventional attack) and cyberterrorism (premeditated action or the threat of such for a variety of political, social, religious reasons). For now the main focus is cyberattacks, namely a term 'that can refer to a range of activities conducted through the use of information and communications technology' (Theohary, 2015: 4). The troubling confusion around this topic and especially that of an act equal to those by "conventional methods", leaves us wondering the role such technology plays in the nuclear deterrence framework. What happens when the two worlds meet, such as the Stuxnet malware

attack on Iranian nuclear centrifuges in 2010? This attack caused the physical destruction of Iranian nuclear material equipment used for refining enriched materials, which if carried out in any other decade would have been an act of sabotage and required a military response. However, because the 21st century offers the perpetrators anonymity via this form of attack, it is almost impossible to justify what would be an appropriate response. Whilst many experts believe Stuxnet was a joint US-Israeli venture to disrupt Iran's nuclear programme (Anderson, 2012), the US itself has said any form of such like attack against themselves, particularly by North Korea will lead them to ‘respond proportionately’ (Theohary, 2015: 1).

I believe this advancement in unconventional warfare undermines the deterrence theory and the non-proliferation regime that both underpins and supports it. The US and Israeli “first-strike” narrative, as well as China's insistent “no first-use” policy are both undermined in a world where they could be the victim of a nuclear attack, without even knowing the party responsible. This 21st century issue also brings to light the frailty of concepts such as “proportionality” in the current world of asymmetric warfare, as this in itself is a normatively constructed idea, which is uncharted in the confines of space and cyber technologies.



Another historic shift in international security is the intelligence industry, and I use the word “industry” purposefully due to the rise in private sector intelligence and security personnel. Intelligence has always been a key aspect of state power and its own form of power in itself, separate but similar in practice to economic or military (Herman, 1996). Intelligence has long been a major organ of a state's power in the world, where once it was ‘circulated as paper’, it is now ‘distributed through multilevel secure electronic databases’ (Aldrich, 2013: 237). This is another development of the 21st Century which poses a risk to the current deterrence theory, namely because the more information at hand, the greater the possibility of it being misinterpreted. This may sound like rather backwards logic assuredly, the more “knowledge” (intelligence-gathering) the better, but perhaps not always. Intelligence gathered by one state via espionage or surveillance, leaves only the receiver of the information to interpret it. Jervis (1976) proposed that preconceptions of various nations, can lead to information being interpreted in a biased manner. The danger posed here is that in this day and age we could apply that theory of preconceptions/ misconceptions to not only nations, but individual actors (i.e. terrorist cell leaders), state-sponsored groups (i.e. al Qaeda), even entire ethnic/religious communities. With the increased ability of modern technology and intelligence institutions, such as the US National Security Agency, to collect enormous amounts of data, surely the mathematical probability of said data being misunderstood also increases.

When you combine an increased potential for simple misunderstandings with the operational readiness of nuclear weapons (the US and Israel famously defend their right to consider a first-strike policy under certain extenuating circumstances), a traditional

deterrence theory appears to get thinner and thinner as it is not evolving with respect to the appropriate change in threat levels of today's security landscape. Another element of 21st century intelligence is the increase in non-state, private actors. The US alone has approximately 2000 private sector intelligence companies, while roughly 'a third of CIA employees are private contractors' (Aldrich, 2013: 237). This globalisation-led shift in the world of intelligence, how it is used and what can be expected of it, mirrors the change from international threats to those of transnational threats. Be it terrorism, clandestine state-backed operations, organised crime or a crime-terror nexus, these threats are no longer identifiable enemies in uniforms assigned to a nation state.

Another contributing factor dating back to the 13th century which has received new attention particularly over Iraq and Syria, is the use of private military contractors (PMCs). There is a large, mostly legal, scale of private contractor roles including those of intelligence operators as mentioned, but also those who provide purely logistical support and training, ranging to armed operational support, in the words of Singer (2001/02). However while various debates rage on as to the legitimacy of states outsourcing military force, it is ultimately a large part of 21st century hybrid warfare. Be it the US Blackwater organisation or the Russian Wagner group, both conceptualize the problem of possessing a nuclear deterrent against unacceptable international acts of aggression. When third-party clandestine troops are at the behest of a mother state, by eliminating any official accountability they undermine formal practices of deterrence. An example being the questionable involvement of Russian-backed Wagner Group soldiers operating in Syria (RBC Magazine, 2016; Grove, 2015), and the consequences should

they have any involvement in another area of potential conflict such as that posed in the western Baltic States. Any severe act of aggression which may lead to nuclear tensions between NATO and Russia would be left wanting, if there is no one to formally "point the finger at".

These changes to the world of 21st century security represent a portion of hybrid warfare, where a nation's enemy can be an individual working from any country with another parties' backing, using transferable skills or information gained from the enormous array of private sector companies, or a group of PMCs used for deniable operations. Is a nuclear deterrent theory that focuses on open dialogue between publicly recognisable figureheads a true safeguard against a world of potentially unidentifiable enemies, which have no intention of identifying themselves or accepting responsibility?

The study into a more complete understanding of deterrence has raised numerous questions when explaining how traditional rationalist accounts of deterrence have been based primarily in exogenously given self-interests of unified actors, stemming from a strong cost-benefit analysis (Price and Tannenwald, 2009). Such questions when problematizing this approach to understanding the validity of deterrence have included; why, in scenarios whereby the threat of retaliation was non-existent, have NW not been used, despite the clear military advantages (E.g. By the US on the non-nuclear state of Iraq during the 1991 Gulf war, despite a small tactical nuclear weapon having clear advantages on this particular battlefield)? The question is then raised as to why certain actors have been more than willing to consider NW use, despite the situation being far from requiring a last resort measure.

President Eisenhower famously reversed the efforts made by the Truman administration to set NW aside as 'something special' to maintain the right to employ them in the future with fewer constraints (Price and Tannenwald, 2009: 13). The relevance of posturing upon these issues is that the 21st century has only furthered the question of what really motivates the deterrence theory. After the Cold War, many argued that realist approaches to international security were insufficient in their understanding and explanatory powers. Others however, believe such mechanisms of change (including developments in weapons of war) do not change the international political structure and its anarchic nature (Waltz, 2000; Wohlforth, 1995), if this is the route of understanding one subscribes to, then the development of NW has not altered the levels of certainty, they have merely added a weapon of mass destruction to a system that is now and always has been, anarchic, uncertain and unpredictable.

Hybrid warfare at its very core promotes uncertainty. The uncertainty of the attacker's identity and the uncertainty of an appropriate proportionate response. Nuclear deterrence and deterrence theory in general however, rely on certainty, certainty that the parties involved are aware of the repercussions and forbade actions, as well as certainty that the retributive acts will be carried out beyond doubt, should the parameters of the unacceptable ever be breached. It is for these reasons that the underlying basis for nuclear deterrence can only be complicated and structurally weakened, as time goes on, with the furtherance of alternative and hybrid warfare.

A small portion of literature has focused its investigation into explaining certain acts of governments as processes of "othering", based

in racism and a need for identity reinforcement as a measure of how to govern in a primarily secular and therefore "uncertain" age (See Mavelli, 2016; Richter-Montpetit, 2014). On the topic of why governments (particularly the US and UK in the "war on terror") still condone torture or "enhanced interrogation techniques", it has been suggested these acts not only give the nation an enemy to explain the presence of evil (a 21st century explanation of secular theodicy), but also reinforces their own "good fortune". In other words, by having a labelled enemy to persecute, we feel more reassured our lifestyle is the correct one. Turning this logic around from an explanation of use into an explanation of non-use, is it possible that in today's world of social media, a plethora of information at our fingertips and heightened public scrutiny, could the current non-use notion of nuclear weapons be put down to a nations image of themselves as not wanting to be perceived as "the bad guys"? Not wishing to attach that particular normative taboo to the identity of its state or citizens, given the undoubtedly 'negative public opinion' that would ensue (Price and Tannenwald, 2009: 15)? If so, the current deterrence based on the NWS possessing up-to-date and over-inflated stockpiles would be irrelevant, as it is not the fear of reprisal that deters, but rather the unwillingness to admit any form of moral weakness or deviance in our characters as rational, civilised actors.

This alternative explanation as to the minimalist role deterrence actually plays in non-use would be supported by the 'profoundly normative concern' (Price and Tannenwald, 2009: 5) that nuclear weapons are simply disproportionate and thus are shunned by the rational and civilised actors that could utilise them, but choose not to.

Conclusion

The 21st century has seen unprecedented and continual changes to the world of international security, shifting focus and traditional norms of rationality away from state-to-state interactions and onto a world of unlabelled and uncategorised uncertainty. Various methods of hybrid warfare such as cyberattacks, PMCs and an increased emphasis of surveillance intelligence, have made anonymity a central feature of modern state interactions, which were previously confined to a small number of espionage and intelligence services. This essay shows how a traditional nuclear deterrence theory based on communication, credibility and capability, against both nuclear attacks and conventional unacceptable acts of aggression or coercion are incompatible with the technology of the 21st century. The 2017 Global Trends Report entitled "Paradox of Progress" (National Intelligence Council) appears to mirror my concerns and assumptions about the current world of security.

Uncertainty about the United States, an inward-looking West, and erosion of norms for conflict prevention and human rights will encourage China and Russia to check US influence. In doing so, their "gray zone" aggression and diverse forms of disruption will stay below the threshold of hot war but bring profound risks of miscalculation. Overconfidence that material strength can manage escalation will increase the risks of interstate conflict to levels not seen since the Cold War (emphasis added, NIC, 2017: 8).

While the current narrative surrounding nuclear deterrence has not changed, the world of international security has. The risk for miscalculations, misunderstandings, disproportionate and potentially misguided

acts of retaliation all will continue to increase in probability.



A Tropospheric Scatter Microwave Radio Terminal (TRC-170) from the 31st Combat Communication Squadron, Tinker Air Force Base, Okla., is positioned in a field during an exercise on May 1, 2012.

Photo Credit: Senior Airman Kenneth Norman/Air Force

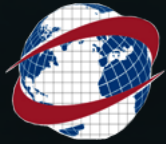
Bibliography

1. Aldrich, R. J. (2013) *Intelligence*. Security Studies. Second Edition (Edited by Williams, P. D.). Oxon: Routledge. 235-249.
2. Anderson, N. (2012) Confirmed: US and Israeli created Stuxnet, lost control of it. *Ars Technica*: Available from <https://arstechnica.com/tech-policy/2012/06/confirmed-us-israel-created-stuxnet-lost-control-of-it/> [Accessed 26/02/17].
3. Byrne, P. (1988) *The campaign for nuclear disarmament*. London: Routledge.
4. Fravel, M. T., Medeiros, E. S., (2010) *China's Search for Assured Retaliation: The Evolution of Chinese Nuclear Strategy and Force Structure*. International Security. MIT Press. 35(2) 48-87.

5. Futter, A., (2015) Trident Replacement and UK Nuclear Deterrence: Requirements in an Uncertain Future. *RUSI Journal*. Routledge. 160(5) 60-67.
6. Grove, T. (2015) Up to Nine Russian Contractors Die in Syria, Experts Say. *The Wall Street Journal*. Available from <https://www.wsj.com/articles/up-to-nine-russian-contractors-die-in-syria-experts-say-1450467757> (December 18, 2015) [Accessed 28/02/17].
7. Herman, M. (1996) *Intelligence Power in Peace and War*. The Classic statement of intelligence and policy. Cambridge University Press.
8. Jervis, R. (1976) *Perception and misperception in international politics*. New Jersey: Princeton University Press.
9. Mavelli, L. (2016) *Governing uncertainty in a secular age: Rationalities of violence, theodicy and torture*. Security Dialogue. SAGE publications. 47(2) 117-132.
10. National Intelligence Council (2017) *Global Trends. Paradox of Progress*. Available from <https://www.dni.gov/files/images/globalTrends/documents/GT-Full-Report.pdf> [Accessed 01/03/17].
11. Nimkar, R. (2009) From Bosnia to Baghdad the case for regulating private military and security companies. *Journal of Public and International Affairs*. 20: 1-24. Available from <https://www.princeton.edu/jpia/past-issues-1/2009/1.pdf> [Accessed 28/02/17].
12. Price, R. & Tannenwald, N. (2009) *Norms and deterrence: The Nuclear and Chemical Weapons Taboos. The Culture of National Security: Norms and Identity in World Politics* (Ed. By Katzenstein, P. J.).
13. Richter-Montpetit, M. (2014) *Beyond the erotics of Orientalism: Lawfare, torture and the racial-sexual grammars of legitimate suffering*. Security Dialogue. SAGE publications. 45(1) 43-62.
14. Ritchie, N. (2014) *Waiting for Kant: devaluing and delegitimizing nuclear weapons*. International Affairs. The royal Institute for International Affairs: Oxford. 90(3) 601-623.
15. Rozhdestvensky, I., et al (2016) Russian private military company 'spotted' in Syria. *Russia beyond the Headlines* (RBC Magazine) Available from http://rbth.com/defence/2016/08/26/russian-private-military-company-spotted-in-syria_624521 [Accessed 28/02/17].
16. Sidhu, W. P. S. (2013) *The Nuclear Disarmament and Non-Proliferation Regime*. Security Studies. Second Edition (Edited by Williams, P. D.). Oxon: Routledge. 409-424.
17. Singer, P. W. (2001/02) *Corporate Warriors: The rise of the privatised military industry and its ramifications for international security*. International Security. 26(3) 186-220.
18. Svendsen, A. (2008) *The Globalisation of intelligence since 9/11*. Cambridge review of International affairs. 21(1): 131-146.
19. Theohary, C. A. & Rollins, J. W. (2015) *Cyberwarfare and Cyberterrorism: In Brief*. Congressional Research Service. Available from <https://fas.org/sgp/crs/natsec/R43955.pdf> (March 27, 2015) [Accessed 20/02/17].
20. Waltz, K. N., (2000) *Structural Realism after the Cold War*. International Security. MIT Press. 25(1): 5-41.
21. Wohlforth, W. C., (1995) *Realism and the End of the Cold War*. International Security. MIT Press. 19(3): 91-129.

By James Morgan

James Morgan is doing his Master's Degree in Terrorism and Society with the School of Politics and International Relations, at the University of Kent, England. His final-year dissertation, entitled "Torture as a Tool of Governmentality: The Relevance of Leaked and Released Visuals of Torture", questions the benefits of disseminating visual information of torture for western liberal-democracies. He plans to pursue a career in security, defence and international affairs.



IRIA


Journal of International Affairs & Politics

Vol. 10

July 2017

Is “Nuclear Deterrence” still
a relevant strategy for the
21st Century?

by James Morgan

© Copyright 2017  IRIA
International Relations Insights & Analysis
All rights reserved.

For more information about IRIA visit:
www.ir-ia.com

Cover Photo: Russian RS-24 YarsSS-27 Mod 2 intercontinental ballistic missiles drive during the Victory Day parade at Red Square in Moscow in May, 2015.
(Photo Credit: RIA Novosti via Reuters)

Back Cover Photo: Sea Sparrow missile is launched from the amphibious assault ship Boxer during a Composite Training Unit Exercise off the California coast.
(Photo Credit: Mass Communications Specialist 2nd Class Kenan O'Connor/Navy)