«MUTUAL ASSURED DESTRUCTION» (MAD)

Umurbaev Rustam Shakirjanovich
4th-year student of Tashkent State University of Oriental Studies
Tashkent city
urustam316@gmail.com
+998946995982

Abstract: *The advent of nuclear weapons fundamentally changed warfare. During the United States and Soviet Union Cold War, both sides developed enough nuclear weapons to destroy each other multiple times over. Each side perceived the other to be a «sensible rational opponent» whose behavior was shaped by «threats of nuclear retaliation» from the other. Each relied upon the other to be concerned about its own survival and to not take an action that would lead to its own annihilation by nuclear retribution. While some secondary and proxy conflicts occurred, neither side could risk deploying a nuclear weapon because of the anticipated response. The «strategic bipolarity» model that defined the Cold War no longer represents the state of the world, in terms of physical conflict.*

Key words: *particular conflict, Cold War, nuclear missiles, significant.*

Introduction

The doctrine of Mutual Assured Destruction (MAD) assumes that each side has enough nuclear weaponry to destroy the other side; and that either side, if attacked for any reason by the other, would retaliate without fail with equal or greater force. The expected result is an immediate irreversible escalation of hostilities resulting in both combatants’ mutual, total and assured destruction. The doctrine further assumes that neither side will dare to launch a first strike because the other side will launch on warning (also called fail-deadly) or with secondary forces a (second strike), resulting in the destruction of both parties. The payoff of the MAD doctrine is expected to be a tense but stable global peace.

The primary application of this doctrine started during the Cold War (1940s to 1990s) in which MAD was seen as helping to prevent any direct full-scale conflicts between the United States and the Soviet Union while they engaged in smaller proxy wars around the world. It was also responsible for the arms race, as both nations struggled to keep nuclear parity, or at least retain second-strike capability. Although the Cold War ended in the early 1990s, the doctrine of Mutual Assured Destruction certainly continues to be in force. Proponents of MAD as part of U.S. and USSR strategic doctrine believed that nuclear war could best be prevented if neither side could expect to survive a full-scale nuclear exchange as a functioning state. Since the credibility of the threat is critical to such assurance, each side had to invest substantial capital in

their nuclear arsenals even if they were not intended for use. In addition, neither side could be expected or allowed to adequately defend itself against the other’s nuclear missiles. This led both to the hardening and diversification of nuclear delivery systems.

Material and Methods

There may be no clear demarcation between peace and war in cyber activities, with different states having different definitions of what constitutes an act of war or a wartime activity – if they have such policies at all. Additionally, the fact that a single armament can have such widely different impacts may result in escalation to nightmare scenarios with widespread impact.

The MAD concept has been applied to cyber warfare in several previous studies. In section cyber warfare was described as warfare involving «cybersecurity, computer network operations, electronic warfare or anything to do with the network». It was defined including actions that attack and protect electronic mediums, as well as attacks and defenses using these mediums. Non-electronic activities related to the foregoing are also inherently included. Morgan, Philbin, Nye, Bendiek, and Metzger propose the adaptation of nuclear era deterrence approaches, based on MAD, to the cyber realm. Lonsdale proposes, in particular, the use of the warfighting approach where (in nuclear deterrence) nuclear weapons were not seen as a complete deterrent solution, but rather as a part of a broader strategy designed to ensure deterrence and post-deterrence-failure capabilities. Crosston, alternately, proposes the concept of «mutually assured debilitation», recognizing that cyber attacks may not destroy (in the immediate way a nuclear detonation would) but can be catastrophically debilitating for cities, nations and their economies.

Results

Ridout proposes a more nuanced strategy adding defense and resilience concepts to the AD-based deterrence concept. Others also have studied and advanced the concept. Chukwudi, Udoka and Charles consider the implications of game theory to deterrence. Davis considers the question of escalation and escalation ladders in the cyber domain. Geers suggests that deterrence may be «an impossible task» due to issues of asymmetry and needing to determine attack attribution, while Gale and Mokarram discuss the use of MAD and deterrence in United States and European strategy, respectively. Huston evaluates factors that may drive J. Straub Technology in Society warfare towards civilian impact, and those that may produce restraint.

This section discusses cyber warfare AD methods and counter-AD methods. It also covers non-AD techniques that can be used to oppose cyber warfare AD techniques. Cyber warfare can be used to implement several different AD methods. Cyber operations can serve as a medium for information and influence operations, as discussed in previous sections. An individual could be contacted, coerced or convinced over electronic channels to take an action that causes significant destruction. This could be through targeted contact or the implementation of a cyber-medium delivered threat or reward targeting the individual. Cyber operations can also be utilized more

directly. The could be used to compromise and electronically command a nuclear weapon or other system that can cause significant destruction directly. Attacking or degrading electronic systems can also be used to cause immediate or long-time-scale damage by preventing communications or other processes required to sustain life.

Discussion

The models presented provide a convenient way to depict and a perspective from which to approach MAD scenario evaluation and the comparison of AD capabilities between individual adversaries in a single medium and across multiple mediums. They also support scenarios where there are two strong alliances and scenarios where there are more than two adversaries, including scenarios with weak and changing alliances. Like any model, though, their greatest weakness is in their reliance on the correct population of information and planners and decision makers, who use the models, having access to all relevant information. Internal controls may obfuscate friendly capabilities. Allies may, similarly, fail to fully disclose their capabilities. Alternately, «fog of war» issues may result in significant over or under estimates of adversary and adversary alliance capabilities. Adversary capability disclosure, pursuant to treaty or other obligations and facilitate facility inspections may be similarly suspect and subject to manipulation.

Given that adversaries and allies alike may have reason to provide incorrect information about capabilities verification of these claims would be highly desirable. However, because cyber capabilities can be developed without the necessity for detectable demonstrations and testing there may be significant potential for misrepresentation. Even activities that are sensed can be problematic, due to issues with attribution. This lack of information can be both beneficial and problematic. It is beneficial because it creates a margin of error, allowing the two sides to have capabilities more divergent than might otherwise be acceptable to prevent one side from feeling that it has the upper hand and attacking. On the negative side, a significant incorrect projection of adversary capabilities may be sufficient to create the same type of scenario where one party believes (incorrectly) that it is in their best interests to attack at present.

Conclusion

This paper has considered the dilemma presented by the existence of multiple AD technologies that have different scopes, immediacy, long term impact and methods of impact. In particular, it has considered how MAD scenarios could play out across multiple domains and mediums and how a MAD scenario could be created from AD technologies from different domains and of different capabilities that are satisfactorily paired to counterbalance the adversary’s own capabilities. Further, this paper has presented models for single domain, two adversary scenarios as well as advanced scenarios where there are multiple domains involved, multiple adversaries and adversaries have multiple capabilities in some or all of the domains. It has described how these models can be used to evaluate, discuss and present work in analyzing MAD.

It also discusses limitations on the models, principally due to their reliance on human input. Future work will include the consideration of the incorporation of non-state actors who possess some AD capabilities and may factor into MAD scenarios, both at present and in the future, into models. Model development that considers issues of attribution and anonymity, including deliberate «false flag» operations is another key area of future work. Further evaluation of the model proposed herein, through its application to relevant scenarios, is also planned.

Acknowledgement

Given the foregoing, while the models provide a framework for considering MAD scenarios and a nomenclature and system of representation for them, they cannot guarantee that the AD capability and MAD comparison calculations are correct in any particular conflict. The quality, completeness and accuracy of the information fed into the models is absolutely critical to ensuring that the answer produced is suitable for decision making.

REFERENCES:

1. W. Curtis The assured vulnerability paradigm: can it provide a useful basis for deterrence in a world of strategic multi-polarity? 16 (3) (2000), pp. 239-256.

2. I. Salehyan The delegation of war to rebel organizations J. Confl. Resolut., 54 (3) (Jun. 2010), pp. 493-515.

3. V. Andre The janus face of new media propaganda: the case of Patani neojihadist YouTube warfare and its islamophobic effect on cyber-actors Islam Christ. Relations, 25 (3) (Jul. 2014), pp. 335-356.

4. J. Forest Perception challenges faced by Al-Qaeda on the battlefield of influence warfare on JSTOR Perspect. Terror., 6 (1) (2012), pp. 8-22.