THE SUBTLE KNIFE: A DISCUSSION ON HYBRID WARFARE AND THE DETERIORATION OF NUCLEAR DETERRENCE

Peter Rautenbach, Simon Fraser University

Abstract

This article looks to tie together the polar opposite of hybrid warfare and nuclear deterrence. The reason for this is that hybrid warfare and its effects on nuclear deterrence need to be explored as there appear to be substantial increases in hybrid warfare's usage. This article found that hybrid warfare has an erosion-like effect on nuclear deterrence because it increases the likelihood that nuclear weapons will be used. This may be due to both the fact that hybrid warfare can ignore conventional redlines, and because the cyber aspect of hybrid warfare has unintended psychological effects on how deterrence functions. How does this relate to nuclear war? In short, cyber warfare attacks key concepts which make nuclear deterrence a viable strategy including the concepts of stability, clarity, and rationality. Therefore, hybrid warfare increases the chance of nuclear use.

Introduction

The world was forever changed when the Trinity Nuclear test occurred. With this initial test, the ultimate destruction of humanity was usurped from the realm of gods into human hands. This advent changed the way society looked at war, but despite this potential for destruction, or perhaps for this very reason, these weapons are some of the best peacekeeping tools humanity has ever attained. The sheer, and assured, level of ruin they could unleash gives nuclear states a defensive advantage and make offensive moves next to impossible. In light of this, a defensive focused world gives stability to the international order. As Robert Jervis put it, "when the defense is dominant, wars are likely to become stalemates and can be won only at enormous cost…raising the costs of conquest to unacceptable levels" (Jervis, 1978, p. 190). When viewed this way, nuclear deterrence has been a key factor in ensuring the continuation of peace between major powers.

Naturally the success of deterrence strategies is difficult to measure as only their failures are blatantly obvious, but nuclear deterrence seems to have been effective as there has been no offensive nuclear use since World War 2. However, the world is not stagnant, and the security situation is constantly evolving. Even weapons of mass destruction cannot change this. While not completely new, contemporary uses of hybrid warfare are causing detrimental erosion on nuclear

deterrence. For this article, the term hybrid warfare will entail a multitude of different short-of-war methods of propaganda, espionage, agitation, cyber-attacks, and the eventual use of nationalist identities and unmarked soldiers to cause disorder and enact favorable change within a state (Lanoska, 2016, p. 179). These "short of war" methods can function separately or in tandem to induce change to the status-quo. Not only does hybrid warfare erode nuclear deterrence because much of it undercuts the uncrossable redlines[1] set by nuclear deterrence, and thus allowing hybrid war to become a useable option of conflict which could incite unforeseen conflict, but also because aspects of hybrid warfare attack key concepts which make nuclear deterrence a viable strategy including the concepts of stability, clarity, and rationality. All three are required for nuclear deterrence to function in manner that successfully deters aggression while simultaneously also ensuring that actual nuclear use is as low as possible. They ensure that while states rely on these weapons, their use would irreparably change the global stage, and thus should only be used as an *absolute* last resort[2]. Therefore, this article will argue that by both eroding the boundaries of deterrence as well as the guiding principles that hold conflict in check, hybrid warfare erodes nuclear deterrence by increasing the odds that nuclear weapons will eventually be used.

This paper is organized into the following sections: first, an exploration of the ties that bind what appear to be the polar opposites of the escalation ladder: hybrid warfare and nuclear deterrence. Following this, the article will delve into the psychological side of the equation and then look at how aspects of hybrid warfare erode the previously mentioned concepts of stability, clarity, and rationality. This second part of the argument will primarily explore the perceived threat from general hybrid warfare and the specific aspect cyber warfare. Both have intangible psychological effects that are detrimental to the viability nuclear deterrence. Finally, this article will demonstrate that hybrid warfare increases the likelihood of nuclear use by simply being a useable form of aggression. This will be achieved by demonstrating a scenario where hybrid warfare could escalate to actual war, thus creating a fertile ground for nuclear weapons use.

[1] Definition of redline in the Cambridge Dictionary is "a limit beyond which someone's behaviour is no longer acceptable" (Retrieved from https://dictionary.cambridge.org/dictionary/english/red-line). When a redline is crossed, a state would theoretically react in an aggressive manner to match the actions taken which crossed their redline.

[2] The use of nuclear weapons against Japan in World War 2 would seem to fly against this statement as they are examples of warfighting using nuclear weapons. For the purposes of this paper, they are not being considered because they are outliers in this discussion as they effectively pre-date or even began, the nuclear age. Once humanity saw what nuclear weapons could do, it can be argued that is when deterrence became a concept.

Definitions and Theory

Before proceeding with this article, key definitions need to be explained and theory explored, specifically the aspects that tie the two key ideas together. It is important to note that, as a strategy, hybrid warfare can be used by both state and non-state actors alike. The definition used earlier does not limit the use of hybrid warfare to any single type of actor. Because the discussion here also revolves around nuclear weapons, this article has a state-based focus. Specifically, there is a focus on Russia and the NATO alliance/United States. However, despite the state based approached taken here, one cannot forget about non-state actors. Effective attribution, or the lack thereof, is a key aspect of hybrid warfare (only in cyber, and only within a specific context). I can have attribution quickly, enough to know who is involved, but not enough to direct the counter cyber strike back at. It will often be the case that one cannot easily determine if a hybrid attack was the work of a non-state actors, a state, or some blurred combination of the two. As it will be seen, even if one can determine some degree of attribution, it is often not enough to warrant a similar type of response. Therefore, while it is often states that will be discussed here, remembering that non-state actors are almost always involved is crucial to exploring hybrid warfare.

Continuing, when looking at both nuclear deterrence and hybrid warfare, one can see that each rest on the metaphorical ladder of escalation, but they occur at different ends. Nuclear warfare has the unlimited potential for destruction, while hybrid warfare often lacks any open aggression. It relies on covert and subversive means to gain an advantage. While the two kinds of warfare are usually considered in separate academic realms, hybrid warfare should be closely studied by anyone who explores nuclear strategy and theory because, unlike real ladders, the ladder of escalation is not a linear structure where each action has a predictable step up or down. Therefore, it is completely possible that hybrid actions could adversely affect nuclear deterrence. The outcome of this combination would be unpredictable at best, and at worst it would be unseen until it was too late to prevent. Before exploring these ideas, an understanding of both terms must first be had.

First, while an incredibly varied strategy, basic nuclear deterrence can be summed up by looking to the theory of Mutually Assured Destruction (MAD). This is the cold, yet effective, logic that nuclear states can never afford to go to war with one another because the retaliation would be too costly. The concept of a "MAD world of deterrable states [posits that] states… are sensitive to costs, clearly perceive other states' interests and intentions, and value conquests less

than others value their independence [and thus] is profoundly peaceful" (Van Evera, 2013, p. 242).

While 'profoundly peaceful' may be a far-off goal for the contemporary world, the fact remains that, despite the ability to engage in wars on an apocalyptic scale, conflict in this way between major powers has yet to occur, and this is arguably due in part to MAD. A key concept here is that the destruction nuclear weapons could create is undeniable. Even the use of a small number of these weapons could devastate states, and this leaves little room from interpretation. No state can ignore this fact. Therefore, states act defensively rather than offensively as "the state that fears attack does not pre-empt-since that would be a wasteful [and dangerous] use of its military resources-but rather prepares to receive an attack. Doing so does not decrease the security of others, and several states can do it simultaneously; the situation will therefore be stable" (Jervis, 1978, p. 190). When the cost of an attack is too great, a degree of stability can exist because every action taken by another state can be assumed, at least to greater degree, to not be aggressive. Thus, nuclear weapons become the ultimate defensive tool.

However, perhaps the most important idea to grasp is the almost certain eventuality that mistakes will be made, and surprises will occur. Furthermore, despite large cuts in nuclear weapon inventories since 1991, the current number of nuclear weapons is approximately 15,000 (Arms Control Association, 2018), and when the inevitable mistake is made, the entire world would be threatened (Kubrick, 1964). Even a "nuclear war between new nuclear states, say India and Pakistan, using much less than 1% of the current global arsenal, could produce so much smoke that… it could produce global environmental change unprecedented in recorded human history" (Robock, 2010, p. 419). Therefore, defendable nuclear deterrence must be much more than simply preventing war. It must ensure the lowest possible chance of nuclear use at all times. This is what hybrid warfare erodes. Not only does it allow for aggressive actions to be undertaken, but it also furthers accelerates crisis-instability. This concept focuses on the fact that despite any apparent advantages one has made in defense, or in the use of 'safe' offensive measures, there has in fact been an increase in the likelihood of miscalculation and the use of weapons of mass destruction (WMDs). The ability to defend or the lack of instability, is what hybrid warfare erodes.

For this article, the term hybrid warfare entails any combination of the different short-of-war methods of propaganda, espionage, agitation, cyber-attacks, and the possible use of nationalist identities and unmarked soldiers to cause disorder and

enact favorable change within a state (Lanoska, 2016, p. 179). While nuclear deterrence revolves around the concept of certainty, hybrid warfare could be described as the antithesis to this certainty. By its very nature, hybrid warfare is designed to be confusing and difficult to pin down. This is both its greatest strength and its greatest danger. Rather than being a new form of conflict, hybrid warfare is a strategy that the belligerent uses to advance its political goals using subversive force instead of blunt conventional aggression (Lanoska, 2016, p. 176). War has always involved far more than the use of kinetic force (Stephen, 2014, p. 361). Millenia ago, the ancient philosopher Sun Tzu wrote on the mental aspects of warfighting and claimed:

> For to win one hundred victories in one hundred battles is not the acme of skill. To subdue the enemy without fighting is the acme of skill. (Sun Tzu, 1963, p. 77)

In the modern world, much of what is call hybrid warfare revolves around new technology such as cyber warfare and usage of these technologies has increased in recent years (Wirtz, 2017, p. 110). These strategies interact with nuclear deterrence by acting as a foil to it. Deterrence is a conservative strategy; it seeks to preserve the status quo and waits on its adversaries before acting (Slantchev, 2005, p. 5). Hybrid warfare is used by actors who recognize the effective inability to alter the status quo through strength of arms. Rather, they conduct short-of-war strategies to go under, and skirt, the redlines presented by deterrence-based powers. The Russian General Valery Gerasimov, a key Russian thinker on hybrid warfare, put forth that the "differences between peacetime and wartime will disappear — war is never declared, and military actions carried out by uniformed personnel and undercover activities will simultaneously support each other" (Holger. M. & Vladimir. S, 2018, p. 319). It is in this idea of constant conflict, or permanent undeclared war, one can see the true danger hybrid warfare poses to traditional nuclear deterrence.

As stated in previous sections, deterrence relies on its certainty. This is the certainty that an aggressive action could be met with a response so great it would negate any gain. However, hybrid warfare counters this strategy as it skirts the line of what warrants a response under traditional nuclear deterrence. This can be seen in the Russia action in Crimea. Former SACEUR General Philip M. Breedlove described the Russia hybrid warfare campaign in Crimea as "the most amazing information warfare blitzkrieg we have ever seen in the history of information warfare" (Vandiver, n.d.). Hybrid warfare often can slip under deterrence measures as it lacks openly aggressive actions, and often tries to

confer an air of legitimacy to its actions. While what happened in Ukraine was an attempt to overthrow the local government, much of it was done through non-aggressive means, such as propaganda, or in a manner that conferred significant deniability to Russia.

This strategy manages to bypass much of deterrence by effectively going under it, thus the certainly that nuclear deterrence can seriously prevent aggression is thrown into question. This is not to say that nuclear deterrence is not preventing more overt forms of combat, but the certainty of deterrence to avert any and all forms of aggression is in question. This crack in certainty in turn creates more fear that aggressive actions will be taken. In Crimea, Putin gambled that the West's desire to avoid nuclear confrontation would allow him to conduct his operations there (Wimmer, 2018). This, combined with the fact that much of what occurred there was done using hybrid warfare, paralyzed the West's ability to deter and react. To this point, both the "EU and NATO have attributed Russia's recent actions in Ukraine to a lack of a forceful response from the West to earlier aggression. Russia learned from its incursion into Georgia in 2008 that it could use military force against non-NATO members in the near abroad without a military response from the West" (Hillison, 2017, pp. 342-343).

The lack of a response from NATO in Crimea fueled the fear of further Russian aggression. It also highlighted the reality that because hybrid warfare allows for potential unchecked aggression where it didn't previously exist, states must plan for this type of incursion. Furthermore, this perception of threat has almost the same effect on states as real threats, especially when it comes to nuclear strategy. Betts noted that states could "stumble into [war] out of misperception, miscalculation and fear of losing if they fail to strike first" (Betts, 2015, para. 14).

In a crisis scenario involving nuclear weapons, stability is paramount, but a fearful state beset by hybrid warfare is unlikely to be stable. The fear of actual aggression can lead to an increased number of mistakes as a state could believe it will be attacked even if this is not true. Hybrid warfare opens the possibility of concrete aggression between superpowers and their allies in way that did not previously exist in the modern world due to nuclear deterrence. It is not simply that it allows states to act aggressively, but rather it creates crisis instability and increases the chances of nuclear use. The idea that hybrid warfare, through the ideas of misperception, could lead to conflict, and then nuclear use is further explored by looking at cyber warfare and how it erodes nuclear deterrence.

Cyber Warfare

This idea of misperception and confusion creating crisis instability is continued when looking at the cyber warfare aspect of hybrid warfare. Earlier in the article it is claimed that hybrid warfare erodes nuclear deterrence; this idea not only revolved around the diminishing effectiveness of nuclear deterrence to prevent combat, but also the fact that hybrid warfare attacks the key aspects of deterrence that allow it to be a useable strategy. At its core, nuclear deterrence revolves around threatening nuclear genocide if attacked.

Furthermore, the destructive level of this threat is so high that it even threatens our existence as a species. To defend such a strategy requires assurance that these weapons would likely never be used. Therefore, in the theory of MAD, actors are assumed to be rational thinkers who can correctly navigate any crisis involving nuclear weapons. While potentially not enough of an assurance to defend nuclear deterrence, a stable environment such as one where there is time to make decisions/assess the attacks intent/determine your own response, which facilitates good decision making is a necessity for nuclear deterrence. To help facilitate good decision making, nuclear weapons are integrated into systems for command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) (Cimbala, 2017, p. 489). These systems work to provide states with the most accurate information, to ensure that each decision is not made under a complete fog-of-war.

Furthermore, to avoid miscalculation and preventable war, states should have the "best possible information about the status of their own nuclear and cyber forces and command systems, about the forces and C4ISR of possible attackers, and about the probable intentions and risk-acceptance of possible opponents" (Cimbala, 2017, p. 489). What all this effectively means is that navigating nuclear deterrence requires reliable information, rationality, and clear thinking (Cimbala, 2017, p. 489). It is these factors that hybrid warfare erodes, with cyber warfare its primary tool of doing so.

While similar in a sense, cyber warfare and its close cousin information warfare are in truth very different from each other. The key difference is that unlike information warfare where effects are often less directed, cyber operations can be used in manner similar to kinetic warfare. Cyber war is a means for reducing the "opponent's" real combat effectiveness; this distorts information and fragments their command-and-control system (Timothy. T, 2014, p. 103). For the

clear majority of world history, defense has always held the advantage (Jervis, 1978, p. 213).

Familiarity with terrain combined with the strength of defensive technology has made securing victory when attacking difficult to achieve. However, "cyberspace as a warfighting domain strongly favors the attacker… [and] this stands in sharp contrast to our historical understanding of warfare, in which the defender has traditionally enjoyed a home-field advantage" (Pyung-Kyun, 2015, p. 387). A cyber-attack allows one to stay in the relative safety of home while causing systemic damage without warning to adversaries. The forms that cyber warfare can take are incredibly varied. They could occur as the crippling of financial markets (Pyung-Kyun, 2015, p. 388), or even the disruption of nuclear command and control systems. While not always damaging in the same sense as conventional weapons, the threat cyber warfare poses to nuclear deterrence cannot be ignored.

As previously mentioned, nuclear weapons are incorporated in C4ISR systems and require reliable intelligence in order to properly deter aggression. Poor intelligence allows for possibility of mistakes, accidental aggression, or miscalculation of enemy intent. Again, this becomes more relevant in a crisis. The crisis scenario is of key importance when discussing nuclear weapons as, unless an egregious technical mistake was to occur, it is in the moment of crisis that the decision to use these weapons would most likely occur. Properly managing a crisis involves "both a competitive and cooperative endeavor between military adversaries… [and] a crisis is, by definition, a time of great tension and uncertainty" (Cimbala, 2017, p. 490). This uncertainty comes from the 'fog of war' that always exists even when intelligence is reliable, and the fact that one can never truly know what the adversary is planning. The fear of attack, of a first strike, permeates every moment during a crisis. Stephen J. Cimbala puts forth that idea that there are four critical requirements to successful crisis management: communications transparency, accurate perception of an adversary's behaviors and motivations, the existence of safety valves so that each side can leave while still saving face, and the reduction of time pressures on actors (Cimbala, 2017, pp. 492-494). These support the core idea that proper nuclear deterrence relies heavily on the psychological concepts of stability, clarity, and rationality. The cyber aspect of hybrid warfare attacks these ideas through either the disruptions of reliable intelligence or through the directly threatening nuclear systems themselves.

A nuclear crisis between two adversaries is not unlike a tense argument where clear communication is key to resolving it peacefully, and cyber warfare often distorts this communication. Thus, cyber-attacks on C4ISR systems could constitute a serious threat to nuclear deterrence. For the Department of Defense, these kinds of attacks would not "be mass destruction… but mass and/or precision disruption" (Cimbala, 2014, p. 283). This would "disrupt, confuse, demoralize, distract, and ultimately diminish the capability of the other side" (Cimbala, 2014, p. 283). An assault like this could take the place of a conventional or even nuclear strike if it was able to successfully disable the ability to use nuclear weapons. However, aside from the conventional-like strike that cyber can perform, its ability to disrupt intelligence is equal in the erosion of deterrence. This disruption of communication can come about in many different forms. An example presented by Cimbala, who has studied cyber warfare and nuclear deterrence in depth, illustrates this point very clearly.

> Suppose one side plants a virus or worm in the other's communications networks. The virus or worm becomes activated during the crisis and destroys or alters information. The missing or altered information may make it more difficult for the cyber victim to arrange a military attack. But destroyed or altered information may mislead either side into thinking that its signal has been correctly interpreted when it has not. Thus, side A may intend to signal 'resolve' instead of 'yield' to its opponent on a particular issue. Side B, misperceiving a 'yield' message, may decide to continue its aggression, meeting unexpected resistance and causing a much more dangerous situation to develop. (Cimbala, 2017, p. 495)

In essence, when information becomes confusing with the intent of misleading one's adversary, the result may not always be what was planned. The result of intelligence disruption is far from certain and could lead to aggressive responses rather than defensive submission. Altering information through the use of cyber warfare to cripple your adversary's ability to utilize their nuclear weapons, in defense or otherwise, will only increase the instability already existent within a crisis. As it was stated before, misinformation is the at the heart of crisis instability. However, it could be possible that rather than targeting a state's intelligence, the true target of a cyber-attack could the nuclear weapon logic controllers themselves. This could be done by severing of communication between leaders and the troops involved in launching nuclear weapons. While negating the ability for commanders to properly command their troops is a powerful strategy, there are again unintended psychological effects that create

further instability and thus are ultimately self-destructive. This takes two different but similar forms.

If communications were severed between command and their troops on the ground, these assets might as well be considered destroyed to a certain degree. For if one cannot give the order to launch their weapons, then their effective warhead count has gone down and their ability to deter has arguably lessened. If one was unable to effectively protect their warheads, they could adopt a 'use them or lose them' policy in which they would have to posture aggressively as they couldn't reliably deter with the threat of a survivable second strike. All of this works to back states into a metaphorical corner because "once either side sees parts of its command, control, and communications system being subverted by phony information or extraneous cyber noise, its sense of panic at the possible loss of military options will be enormous" (Cimbala, 2017, p. 495). This panic and perceived urgency then also limits the options available to actors as they believe they could be facing an imminent nuclear strike.

In order to navigate the way through a crisis scenario, both time and space are required. Imagine a scenario where President Kennedy had lacked the required time need to push the discussion in the Cuban missile crisis away from air strikes and invasion. The crisis could have very well ended in tragedy (Cimbala, 2017, p. 497). Therefore, the disruption of communication through hybrid warfare has the added effect of increasing crisis instability through the creation of confusion. However, the confusion from disruption not only affects leaders, but the commanders on the ground as well. Often there is a certain degree of autonomy given to commanders when it comes to using nuclear weapons. This is done to create some redundancy and resilience in the state's nuclear deterrent option.

This idea has been seen, albeit somewhat differently, during the Cold War in mainland Europe. At the time, the U.S. was faced with the conventionally armed superior USSR who could have pushed through NATO forces. To stop that from happening, theorists such as Robert Jervis put forth the idea of 'The Threat That Leaves Something to Chance' (Christensen, 2012, p. 450). The core concept here was that if the U.S. were to deploy nuclear weapons to the frontlines there was the chance that, in the event of a Soviet invasion, they would be fired, and this meant that the USSR could never be completely sure that a conventional attack wouldn't escalate to all out nuclear war (Christensen, 2012, p. 466). This was again due to the fact that commanders on the ground, in charge of nuclear weapons, often had orders to use them if under attack. With this in mind, the

USSR couldn't attack mainland Europe and thus the Cold War continued its trend of no open warfare directly between the two powers.

While this strategy is primarily about deterring a superior conventional force, the key idea is that, under certain circumstances of attack, commanders on the ground could launch their nuclear weapons without new orders from on high. While these exact conditions are highly classified, it is reasonable to assume that cyber disruption could trigger this kind of a launch. As cyber-attacks on nuclear weapons can have a similar effect to a kinetic strike on them, and could appear, at least as far as the command knows, to be the first sign on an all-out attack, nuclear weapons could theoretically be launched. NATO also "[recognized] cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea" (NATO, Last Updated–2017, Section 70). This falls back onto the 'use them or loss them' idea presented earlier. Furthermore, if the communication between leaders and those on the ground who launch these weapons is disrupted then no command could stop the launch[3]. The old adage of cutting the head off the snake then becomes uniquely dangerous in a nuclear crisis. Therefore, through cyber warfare, hybrid warfare again erodes deterrence by impacting the psychology of those use nuclear weapons to deter aggression ultimately adding to crisis instability and increasing the chance of nuclear use.

The Dangers that come from Hybrid Warfare's Usability

Cyber warfare is not the only aspect of hybrid warfare that erodes nuclear deterrence. As it was previously stated, a key part of deterrence is that the very weapons used to deter aggression should never be fired until it is the last resort. Furthermore, it was posited that one of hybrid warfare's greatest strengths is that it undercuts the usual redlines set by nuclear deterrence. This is again because hybrid warfare lacks the traditional markers of conventional attacks, death, and destruction. However, while this is true, this isn't to say that hybrid threats shouldn't be taken as seriously as conventional ones. This is due to the ladder of escalation. Any form of conflict can escalate into something more then was initially planned. Therefore, any weapon that it thought to be free of consequence,

[3] It should be mentioned that there have been many cases where individuals could have launched nuclear weapons. (Aksenov, 2013) These often occurred due to technical issues or communications failure. The bravery and level headedness of these individuals prevailed, and no weapons were fired. However, this does illustrate the point that errors can occur, and it was only with great luck that those individuals were present at the time.

and therefore easily used, is truly a great threat. For each time of conflict, the metaphorical dice is cast, and the potential of escalation there.

Hybrid warfare is the prime example of such a weapon where one can attack with a perceived lack of consequences. This was the case in Crimea where Russia was met with very little true resistance from the international community. The real question is, fueled by their success in Crimea, if Russia were to attempt the same sort of operations in a NATO member state, what would the result be? The following scenario explores how Russian hybrid warfare against NATO could realistically unfold and puts forth that hybrid warfare could escalate to a nuclear exchange[4].

The Use of Hybrid Warfare and the Misperception of Easy Victory

As an alliance, the cornerstone of NATO's responsibility is the collective defense of its allies (NATO, Last Updated-2018). In the conventional context, NATO has no match. Alone, the military spending in the U.S is at $598 billion while Russia rests at $66 billion (Karklis and Taylor, 2016). While spending levels aren't the sole determining factor in a conflict, they do indicate a greater ability to provide better technologies or more well-trained soldiers. Furthermore, in the nuclear arena, despite having approximately 7000 nuclear warheads (Kristensen and Norris, 2018, p. 185), Russia cannot gain an easy advantage due to the assured level of destruction one would expect/predict as explained by MAD. In this light, NATO's ability to deter Russia from ever openly attacking them is relatively secure, however, "the boundaries between… regular and irregular warfare are blurring… and states will increasingly turn to unconventional strategies to blunt the impact of American power" (Boot, 2006, p. 200).

While the situation in Ukraine will not exactly be replicated in NATO, the threat of hybrid warfare is very real for the Baltic states. These states demonstrate a few key requirements for being prime targets of hybrid warfare. To begin with, they are home to fractured ethnic and linguistic groups which are primarily Russian in nature. These ties confer an informational advantage to Russia, as it gains a better understanding of local rivalries and grievances (Lanoska, 2016, p. 189). Furthermore, because the Baltic states are not particularly strong states, they are unable to mend these grievances and this allows them to be manipulated by

[4] This scenario comes from previous paper written from this author (Peter Rautenbach) that explored how the usability of hybrid warfare, and the assumption of being able to use it without a punishing response could trip states into war, and even nuclear conflict. It is being discussed here as it is a prime example of how hybrid warfare increases the chances of nuclear war.

belligerents such as Russia (Lanoska, 2016, p. 189). Therefore, they are vulnerable to the use of subversive hybrid warfare by Russia, and despite their protection under Article 5, it is unclear what NATO could do to deter and defend against this form of aggression (Lanoska, 2016, p. 175).

This situation seems to indicate that, not only could Russia potentially see success in their effort to conduct hybrid warfare in the region, but that they might be able to do so without serious repercussions. However, while it is true that there is difficulty in responding to hybrid warfare, any hope that NATO would fail to respond is misplaced. Van Evera placed false hope at the center for his theories on the causes of war, and hybrid war is a prime example of this concept. For him, "war is more likely when states fall prey to false optimism about its outcome" (Van Evera, 2013, p. 14). This is all a matter of perception, and if states believe that they can achieve victory, then they will attempt to gain it. Of course, most of the worst wars in human history have started as a result of misperception.

In World War One (WWI), there was the misperception that offensive action would lead to easily achieved victory, but it was defensive technology that was superior, and this mistake directly led to the prolonged nature of World War One (WWI)I and thus caused it to be one of the bloodiest wars in history (Jervis, 1978, p. 191). The opposite is true for World War Two (WWII). Due to the defensive nature of the WWI, it was believed that after WWI there was once again a defensive advantage. This was again a case of misperception that led to conflict. New technology improvements in tank and airplane technology combined with tactical innovations such as the Blitzkrieg had in fact created an offensive advantage (Jervis, 1978, p. 191). If states had correctly perceived this advantage perhaps the outbreak of WWII could have been prevented. The danger of hybrid warfare is that is appears to circumvent traditional aggression and therefore it could add a false air of confidence to states. When considering the ladder of escalation, any strategy that makes war easier and more likely is dangerous.

NATO, Article 5, and Responding to Hybrid Warfare

To maintain the security of member nations, there are two scenarios where NATO would respond to hybrid warfare. The first of these focuses on the possibility of Russian forces being deployed as unmarked militia within NATO states. The first steps of hybrid warfare have been described as covert in the sense that they focus on the use of short-of-war strategies which aim to destabilize a country. These can take many forms and such tactics could include information warfare, cyber warfare, and the use of criminal activities. These are designed to

add an element of chaos to a state and weaken its ability to respond to the next stage which could involve nationalist uprisings.

If the state of affairs within a NATO ally followed this destabilizing trend, and even involved a civil war and armed conflict, it is plausible to assume NATO could get involved in some capacity and Article 5[5] could be invoked. This idea was codified in the latest NATO summit in Warsaw, as NATO declared that it was "prepared to assist an ally at any stage of a hybrid campaign, [that] the Alliance and Allies will be prepared to counter hybrid warfare as part of collective defense, [and that] the Council could decide to invoke Article 5 of the Washington Treaty" (NATO, Last Updated-2017, Section 72).

Aside from the danger that any conflict brings, the later stages of hybrid warfare in Ukraine involved the use of unmarked Russian troops as militia. If this pattern were repeated in a Baltic conflict, then a NATO intervention would mean a direct confrontation with Russian troops. While it is difficult to say where the situation would exactly go at this point, nonetheless NATO and Russian troops could be engaged in conflict, and this could lead to escalation out of simple hybrid warfare and into the conventional realm.

There is also the fact that NATO could respond to any cyber operation conducted against the alliance. While the unintentional psychological effects of cyber warfare and how it erodes nuclear deterrence has already been discussed earlier in this article, cyber warfare also has a part to play in this scenario. In that section, it was put forth that cyberattacks on a state's nuclear deterrence apparatus could trigger a retaliatory strike. This certainly points to the danger of cyberattacks, and how even something simply meant to confuse or destabilize could trigger nuclear use. However, directly targeting nuclear weapons and their command structure isn't the only way cyber warfare could lead to actual conflict. If a NATO member state were struck by a cyber-attack that mirrored a conventional strike, it is plausible that this could trigger Article 5 and to an extension, a military response.

While NATO does recognize cyberspace as a domain of operations, similar to air, land, and sea" (NATO, Last Updated-2017, Section 70), the exact time a cyberattack merits a hard power response is not easy to determine. Like the clear majority of hybrid warfare, the ambiguity of cyber-attacks makes responding difficult and often disproportionate. During a NATO military exercise in 2010 in

[5] Article 5 is a provision within the NATO treaty that stipulates that an attack on one member nation is an attack on all. If used, all other members will join their ally in the conflict.

which a sophisticated cyber-attack was simulated, it "became apparent that no one 'could pinpoint the country from which the attack came" (Markoff et al, 2010). On the other hand, "the US could quickly attribute the 2014 Sony attack to the North Korean State, and the recent hacking of the Democratic National Committee has been attributed to the Russian State" (Stockburger, 2016, p. 578).

Attribution is a possibility. The question that remains is that if an attack could be attributed, when would it merit an Article 5 level response? A test development by Professor Michael Schmitt was designed to determine when a cyber-attack amounted to a use of force. The conditions it set are: "(1) severity; (2) immediacy; (3) directness; (4) invasiveness; (5) measurability of effects; (6) military character; (7) State involvement; and (8) presumptive legality" (Schmitt, 1999, 903). While all of these are important in determining when to respond, the first factor - the severity of an attack, is perhaps the most important. While the 2007 attack on the Estonian financial institution was undoubtedly both a use of force and a breach of sovereignty, it would be difficult to defend the use of NATO military force in response. On the other hand, if this attack had instead targeted a power grid, knocking out power for hospitals and resulting in the deaths of patients, a NATO response would have been far more likely. However, even in this scenario, there is serious doubt as to how NATO would respond. It was recently revealed "that hundreds of deaths a year could be caused by computer problems" (Pickover, 2018) in the National Health Service. Furthermore, they put forth that "WannaCry ransomware attack - which crippled parts of the NHS last year – 'could have killed a lot of people'" (Pickover, 2018).

The WannaCry ransomware attack has been blamed on North Korea by many states including the US and the UK (BBC, 2017). Despite this apparent attribution to a state, there has not been much of a response by NATO. This could be due to the issue with the measurability of deaths caused by the WannaCry attack and the fact that while faulty computers appear to have caused these deaths, the specific number of those directly linked to North Korea is unknown. Furthermore, the attack on the hospital appears to have not be targeted but an unintended casualty once the attack was released on the globe. The circumstantial and vague nature of the attribution and scattered nature of the targeting undercut the ability to respond to the WannaCry attack. Nonetheless, the difficulty that comes with properly responding to a cyber-attack should not distract from properly exploring the possibly of a respond. There are real scenarios where a response does appear possible, especially if the attacked states called for NATO support. Naturally, all of this is hypothetical, but as boundaries are pushed and probed, eventually something will push back.

Russian Reaction to a NATO Response

In all, it appears very clear that there are many cases of hybrid warfare to which NATO would ultimately respond with military force. How this would exactly unfold is hard to predict, but the alliance's resolve can't be ignored. Therefore, it is reasonable to assume that hybrid operations against NATO could in fact escalate to conventional conflict. The final question is how Russia would react if NATO forces encountered Russian militia or military personal during hybrid operations. This is where nuclear weapons enter the equation. As previously mentioned, these types of operations are undertaken by those who want to change the status-quo but cannot due so openly. NATO's vast military might, combined with nuclear deterrence, be primarily why Russia has increased its usage of hybrid warfare.

Russia has also adopted lower thresholds for the use of nuclear weapons. Russia lacks both the ability to enact favorable change against the status-quo, or as well as combat threats from NATO, and therefore they needed to adapt. Within Russia, "military leaders have openly stated that Russia has deliberately lowered the nuclear use threshold and talk about the use of nuclear weapons in regional and local wars" (Schneider, 2008, p. 397). A regional or local war could easily mean a conflict in the Baltics. This indicates an increased reliance on nuclear weapons for Russia as they are being assigned to situations where conventional weapons were once the answer.

The weapons that would be used in the face of American conventional power would be the smaller tactical nuclear weapons which are intended for battlefield use and have at most 100 tons of TNT in explosive power (Schneider, 2008, p. 397). While this doesn't come close to rivaling the explosive power used in Hiroshima, a single one of these weapons would drastically alter any battlefield. This is known as the Russian policy to 'escalate to de-escalate'. This policy is comparable to MAD except that where MAD threatens unacceptable damage, de-escalation through limited nuclear strikes "provides instead for infliction of 'tailored damage' [which is] defined as damage [that is] subjectively unacceptable to the opponent [and] exceeds the benefits the aggressor expects to gain as a result of the use of military force" (Sokov, 2014).

While the immediate explosion would be devastating, the real risk is that of further escalation. The first use of nuclear weapons is a potential existential threat as most states have doctrines that demand that they then respond in kind to prevent further use by adversaries. These doctrines were designed to only

threaten nuclear use so that these weapons would never be truly used, but as in this example, they might be forced to demonstrate their resolve and prove their deterrent is credible. For if one doesn't respond when their deterrent demands, then how credible is their deterrent? It is technically possible that each side would exchange nuclear warheads in a limited manner, leading to a great risk of further nuclear escalation.

With this scenario in mind, one can see how the usability of hybrid warfare, and the misperception of a lack of response, could 'trip' states into conflict. This demonstrates another way in which hybrid warfare can unintentionally contribute to crisis instability. By its very nature hybrid warfare creates instability, and because of the possibly misperceived inability of NATO to respond, it is a real danger to nuclear deterrence. This misperceived inability to respond to hybrid warfare is what erodes the ability of states to properly use deterrence as a strategy. If Russia were to attempt to replicate their success in Ukraine against a NATO member states, there is a realistic path of escalation that goes all the way to nuclear use. Therefore, because it is perceived to be a useable weapon which is free from reproach, hybrid warfare increases the chance of nuclear use.

Conclusion

This article sought to tie together the two concepts of hybrid warfare and nuclear deterrence. In doing so, it put forth that aspects of hybrid warfare, more specifically cyber warfare, directly erode the viability of nuclear deterrence as a strategy. When states use nuclear weapons to deter aggression, they are effectively threatening genocide. While terrible, it could be the situation that this destruction is possibly preferable to world devoid of nuclear deterrence. Be careful Regardless, putting aside any debate on this cold logic, deterrence must have a limit.

The entirety of the world should never be threatened for the safety of one's state. This is a cost to high to pay. Hybrid warfare erodes both the boundaries of deterrence as well as the guiding principles that hold conflict in check, thus corrodes nuclear deterrence by increasing the odds that nuclear weapons will eventually be used. Therefore, one can never ignore even the seemly short-of-war strategies because they increase crisis-instability. In a sense they act as a subtle knife that attacks deterrence with a thousand shallow cuts. Sowing misperception and confusion in their wake. Shallow or not, anything that erodes deterrence must be looked at with the upmost scrutiny. Humanity only has one planet, and it is our responsibly to safeguard it from threats such as these.

References

Aksenov, Pavel. (2013). Stanislav Petrov: The man who may have saved the world. Retrieved from https://www.bbc.com/news/world-europe-24280831

Arms Control Association. (2018). Nuclear Weapons: Who Has What at a Glance. Retrieved from https://www.armscontrol.org/factsheets/Nuclearweaponswhohaswhat

BBC. (2017). *Cyber-attack: US and UK blame North Korea for WannaCry.* Retrieved from https://www.bbc.com/news/world-us-canada-42407488

Betts, R. K. (2015) Realism Is an Attitude, Not a Doctrine. *The National Interest*. Retrieved from https://nationalinterest.org/feature/realism-attitude-notdoctrine-13659

Boot, M. (2006). *War Made New*. New York: Gotham Books.

Christensen, T. J. (2012). The Meaning of the Nuclear Evolution: China's Strategic Modernization and Us-China Security Relations. *The Journal of Strategic Studies,* 35(4), 447-487.

Cimbala, S. J. (2014) Cyber War and Deterrence Stability: Post-START Nuclear Arms Control. *Comparative Strategy,* 33(3), 279-286. doi: 10.1080/01495933.2014.926727

Cimbala, S. J. (2017). Nuclear Crisis Management and Deterrence: America, Russia, and the Shadow of Cyber War. *The Journal of Slavic Military Studies,* 30(4), 487-505. DOI: 10.1080/13518046.2017.1377007

Hillison, J. R. (2017). Fear, Honor, and Interest: Rethinking Deterrence in a 21st Century Europe. *Orbis*, 61(3), 340-353. DOI : 10.1016/j.orbis.2017.05.005

Holger, M. & Vladimir, S. (2018). Information Warfare as the Hobbesian Concept of Modern Times — The Principles, Techniques, and Tools of Russian Information Operations in the Donbass, *The Journal of Slavic Military Studies,* 31(3), 308-328, DOI: 10.1080/13518046.2018.1487204

Karklis, L., & Taylor, A. (2016). This remarkable chart shows how U.S defense spending dwarfs the rest of the world. Washington Post. Retrieved from https://www.washingtonpost.com/news/worldviews/wp/2016/02/09/this remarkable-chart-shows-how-u-s-defense-spending-dwarfs-the-rest-of-theworld/?utm_term=.3beb7b49e20f

Kristensen, H. M., & Norris, R. S. (2018). Russian Nuclear Forces, 2018. *Bulletin of the Atomic Scientists*, 74(3), 185-195. DOI: 10.1080/00963402.2018.1462912

Kubrick, S. (1964). *Dr. Strangelove or: How I Learned to Stop Worrying and Love the Bomb* [Motion picture, VHS]. Columbia Pictures.

Lanoska, A. (2016). Russian hybrid warfare and extended deterrence in eastern Europe. *International Affairs*, 91(3), 175-195.

Markoff, J., et al. (2010). In Digital Combat, U.S. finds No Easy Deterrent. N.Y. TIMEs. Retrieved from http://www.nytimes.com/2010/01/26/world/26cyber. html.

NATO. (Last Updated - 2018). Collective Defence - Article 5. North Atlantic Treaty Organization. Retrieved from http://www.nato.int/cps/en/natohq/topics_110496.htm.

NATO. (Last Updated - 2017). Warsaw Summit Communiqué. North Atlantic Treaty Organization. Retrieved from http://www.nato.int/cps/en/natohq/official_texts_133169.htm

Pickover, E. (2018). NHS computer problems could be to blame for ‘hundreds of deaths’, academics claim. Retrieved from https://www.independent.co.uk/news/health/nhs-computer-problems-blamehundreds-deaths-harold-thimbleby-martyn-thomas-gresham-collegea8197986.html

Pyung-Kyun, W. (2015). The Russian Hybrid War in the Ukraine Crisis: Some Characteristics and Implications. *The Korean Journal of Defense Analysis*, 27(3), 383-400.

Robert, J. (1978) Cooperation Under the Security Dilemma. *World Politics*, 30(2). 167-214.

Robock, A. (2010). Nuclear Winter. WIRE;s Climate Change, 1. 418-427, DOI: 10.1002/wcc.45.

Schmitt, M. N. (1999) Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework. *The Columbia Journal of Transnational Law, 37.* 885-937.

Schneider, M. (2008) The Nuclear Forces and Doctrine of the Russian Federation. *Comparative Strategy,* 27(5) 397-425, DOI: 10.1080/01495930802430098

Slantchev, B. L. (2005). Introduction to International Relations: Lecture 8: Deterrence and Compellence. 1-4. Retrieved from http://slantchev.ucsd.edu/courses/ps12/08-deterrence-and-compellence.pdf

Sokov, N. N. (2014). Why Russia calls a limited nuclear strike 'de-escalation'. *Bulletin of the Atomic Scientists*. Retrieved from http://thebulletin.org/whyrussia-calls-limited-nuclear-strike-de-escalation

Stephen, C. J. (2014) Sun Tzu and Salami Tactics? Vladimir Putin and Military Persuasion in Ukraine, 21 February–18 March 2014. *The Journal of Slavic Military Studies*, 27(3), 359-379, DOI: 10.1080/13518046.2014.932623

Stockburger, P. Z. (2016). Know Unknows: State Cyber Operations, Cyber Warfare, and the Jus Ad Bellum. *American University International Law Review,* 31(4), 545-591.

Sun Tzu. (1963). *The Art of War*. Griffith, S. B (ed. & trans). New York: Oxford University Press.

Timothy, T. (2014). Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts? *The Journal of Slavic Military Studies*, 27(1), 101-130, DOI: 10.1080/13518046.2014.874845

Van Evera, S. (2013). *Causes of War: Power and the Roots of Conflict.* London: Cornell University Press.

Vandiver, J. SACEUR: Allies Must Prepare for Russia 'Hybrid War'. Star and Stripe. Retrieved from, http://www.stripes.com/news/saceur-allies-must-prepare-forrussia-hybrid- war-1.301464.

Wimmer, F. (2018). European nuclear deterrence in the era of Putin and Trump. *Bulletin of the Atomic Scientists*. Retrieved from https://thebulletin.org/2018/01/european-nuclear-deterrence-in-the-era-ofputin-and-trump/

Wirtz, J. J. (2017). Life in the "Gray Zone": observations for contemporary strategists. *Defense & Security Analysis*, 33(2), 106-114, DOI: 10.1080/14751798.2017.1310702

Published by the Journal of Intelligence, Conflict and Warfare and Simon Fraser University

Available from: https://jicw.org/