OPEN PUBLICATIONS

Hedging and Risk Acceptance in Future Warfare across Domains

Volume 9, Number 2, 2024

ISSN 2957-7160 (Online)
ISSN 2957-7799 (Print)

DISCLAIMER:

Let us know your thoughts on
"Hedging and Risk Acceptance in Future Warfare Across Domains"
by emailing us at: ***editor@openpublications.org***
www.openpublications.org

CREDITS

CONTRIBUTING AUTHOR

Dr. Oktay F. Tanrısever, Professor of International Relations
at the Middle East Technical University (METU), Ankara-TÜRKİYE

OPEN CAPABILITY LEADER

Col Stefan Lindelauf

OPEN LEAD EDITOR

Dr Mehmet Kınacı

OPEN OPERATIONS MANAGER

LTC Alexios Antonopoulos

ACTION OFFICER

Maj Asım Kemal Cömert

OPEN EDITORIAL REVIEW BOARD

LtC Ferenc Pasztor
LtC Tor-Erik Hanssen
Cdr Silvio Amizic
Cdr Alban Morel
Cdr Alan Cummings
Ltc Dirk Mathes
Maj Mithat Almaz
Dr Jonathan White
Mr Helmar Storm
Ms Klodiana Thartori

TECHNICAL EDITOR

Dr. Maureen Archer

ART DESIGNER

PO1 Elizabeth Denys

CONTENTS

EXECUTIVE SUMMARY

All strong security strategies differ from weaker ones in their capacity to differentiate between significant and not-so-significant security risks. Therefore, international security actors as well as their security alliances, such as NATO, should manage their security risks strategically through hedging certain significant security risks and accepting the others as not-so-significant security risks. In the increasingly complex international environment with hybrid characteristics of future warfare and increasing integration and networking trends across domains, international security risk management becomes increasingly more difficult. Thus, international security actors need to make their decisions about hedging and risk acceptance more strategically and systematically so they can make more resilient and agile international security plans to counter their rivals.

This research paper argues that in constantly shifting international security contexts, effective responses to the challenges of hedging or accepting international security risks require the adoption of a dynamic, systematic, and strategic assessment of the strengths and weaknesses of the international security actors. Likewise, assessments are needed of emerging opportunities and threats across domains, where the social, technological, environmental, economic, and political factors disrupt and reshape strategic environments. Therefore, to enhance their proactive, agile and resilient risk management strategies, all international security actors need to develop more effective international security risk communication strategies towards their stakeholders with increasingly diverse interests and perceptions.

The paper also suggests that international security risk management strategies should be flexible enough to adjust swiftly to the challenges of diverse forms of warfare. These strategies should also be flexible enough to strengthen their own strategic situational awareness regarding the interconnections among the major domains of military activity. The organizational structure and strategic thinking of international security actors should also demonstrate more adaptability to the rapidly changing strategic environment in which they operate. This requires them to adopt an ever-dynamic 360-degree approach rather than a static and limited approach. Such a dynamic approach is needed toward shifts not only in the capabilities, interests and intentions of their rivals but also in their own organizational and opportunity structures, as well as in their strategic responses to the international security challenges ahead.

Keywords: Strategic Risk Management, Hedging, Risk Acceptance, Future Warfare, Situational Awareness, Across-Domain Operations

INTRODUCTION

All international security actors, referring to state and non-state actors -such as international organizations and regional security alliances- that have significant capacity to influence international security situation, make their military planning in order to win a potential future war. However, it is always uncertain if they could win a potential war, since the military and non-military strengths of the warring sides can be tested against each other only when they actually start fighting. This makes the military preparedness of the sides a decisive factor in shaping the outcome of a future war. One of the crucial aspects of military preparedness is the existence of a superior military plan that allocates strategic resources for coping mainly with the strategically significant security risks rather than dealing with all security risks. Thus, a superior military plans categorize security risks into strategically important and strategically less important risks realistically.

Recognizing the significance of international security risk management, this paper explores the key features of dynamic hedging and risk acceptance responses of international security actors in future warfare contexts across all domains. The paper also identifies the main security challenges posed by the adoption of ineffective risk management strategies during future across-domain warfare.

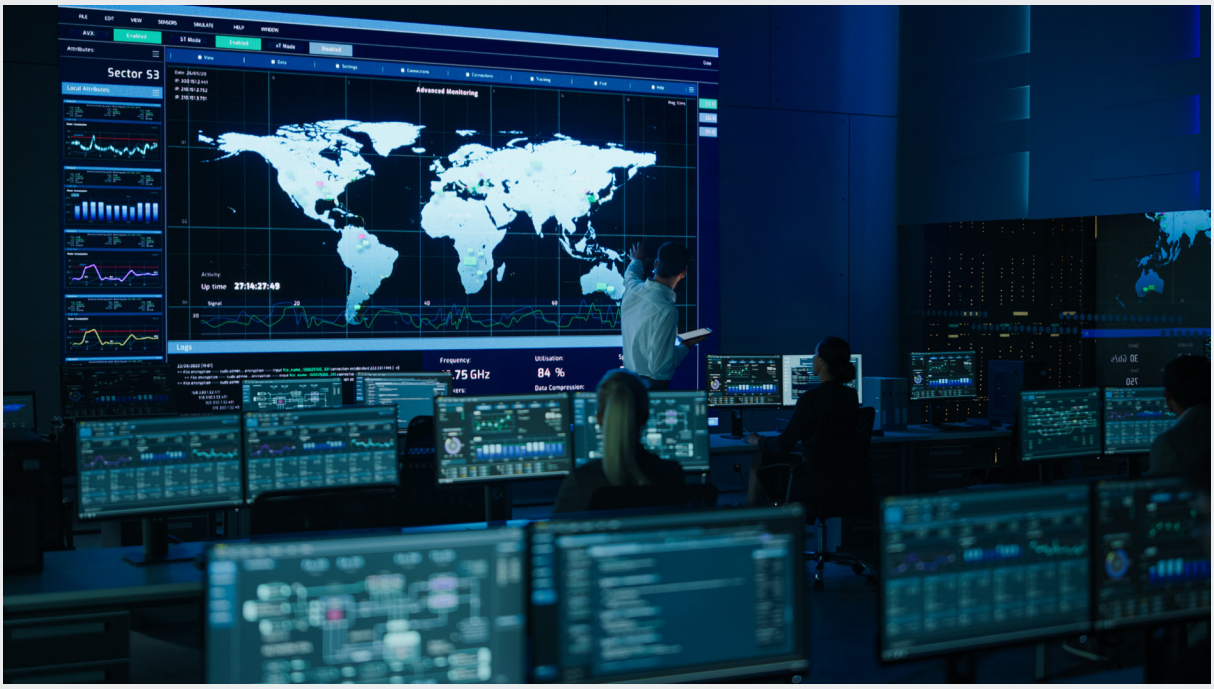
Methodologically, the paper benefits from SWOT (Strength, Weakness, Opportunities and Threats) as well as the STEEP (Social, Technological, Environmental, Economic and Political) analytical frameworks for understanding NATO's decisions on evading or accepting specific security risks emanating from the future warfare across domains. Accordingly, the findings and conclusions are based on a detailed analysis of relevant books, articles, blogs and security think-tank reports about managing security risks of the future across domains warfare contexts. To this purpose, a 360-degree approach was adopted regarding the key formal and informal as well as theoretical and policy-oriented security debates on the ways of managing international security risks in future warfare contexts across domains.

The paper is organized as follows:

A. Conceptual Framework: Security, Threat, Risk, Hedging, and Risk Acceptance. The first section develops a conceptual framework through which the concepts of security, threat, risk, hedging, and risk acceptance are put into a theoretically coherent strategic perspective.

B. Dynamic vs. Static Risk Assessment Models for Hedging and Risk Acceptance Decisions. The second section explores the characteristics of a dynamic and strategic risk management approach for deciding whether to hedge or accept international security risks.

C. Hedging and Risk Acceptance Responses to the Challenges of Future Warfare. The third section discusses the characteristics and challenges of by exploring the strengths, weaknesses, opportunities and threats that future warfare could create for international security actors.



D. Managing Security Risks in the Complex Strategic Environment of Future Cross-domain Warfare. In this section, the paper provides an international security risk assessment of the trends in the social, technological, economic, environmental and political contexts as well as the hedging and risk acceptance options of international security actors in waging future wars across the land, maritime, air, space, and cyberspace domains of military activity.

E. Recommendations for NATO. In the following fifth section, the paper proposes three actionable policy recommendations for NATO in order to enhance its capacity to become a more resilient and agile "shared risks security community".

The paper concludes by highlighting its key findings and conclusions regarding the hedging and risk acceptance responses of international security actors.

A. CONCEPTUAL FRAMEWORK: SECURITY, THREAT, RISK, HEDGING, AND RISK ASSESSMENT

The concepts of hedging and risk acceptance are closely related to the concepts of risk and threat which play a constitutive role in the conceptualization of security. Therefore, the way in which the central concept of security is defined significantly shapes the conceptualization of its derivatives, such as threat, risk, hedging, and risk acceptance.

Security has been considered one of the most central concepts of social sciences. In the field of international relations, Arnolds Wolfers developed one of the widely used definitions of security conceptualization. According to Wolfers, security means a situation where threats to our acquired values are deterred, countered, or neutralized. More precisely, for Wolfers, security, in an objective meaning, signifies "the absence of threats to acquired values", while in a subjective meaning, it stands for "the absence of fear that such values will be attacked" (Wolfers, 1962, p. 150).

In most conceptualizations of security, the concept of threat plays a decisive role in shaping the meaning of security, even if 'threat' remains one of the ambiguous and essentially contested concepts, like the concept of security. In fact, Wolfers' conceptualization of security suggests that some of the objectively verifiable 'threats' to our acquired values may not be perceived by people as 'threats'. Likewise, some of the subjective perceptions of 'threats' may be held popularly by the people, but their existence cannot be established objectively (Wolfers, 1962: 147-165).

The centrality of the concepts of 'threat' and 'risk' in the conceptualizations of security stems from the fact that security is something always relational and exists always to a certain degree. Although all international actors adopt various strategies to maximize their security, they cannot enjoy 'total security' since all international actors have little or big vulnerabilities to the existing or potential 'threats' (Buzan and Waever, 1998). In this sense, the concepts of 'threat' and 'vulnerability' are closely linked, as 'threat' refers to any offender that is capable of taking advantage of one's existing 'vulnerability', which in turn refers to a weakness which could be manipulated by various actors (Eriksson, 2001).

In fact, the vulnerabilities to the existing 'threats' and future 'risks' stem from the 'security dilemma' which is an inherent attribute of security policies of all actors, since any improvement in the perceived or real security conditions of any international actor or security alliance could motivate the others to take some counter-security measures so that security vulnerabilities of all international security actors continue to exist (Jervis, 1978: 167-214). As some of the threats and vulnerabilities cannot be addressed completely, rather than total security, an adequate or satisfactory level of security has been considered acceptable or tolerable by all security actors (Jervis, 1985).

International security actors perceive security 'risks' when their existing level of security is perceived to be threatened by a likely future situation. Such security risks could emanate from both external and internal factors such as geopolitical rivals, international trade restrictions, and the actors' own poor responses to external challenges. In this sense, 'risk' seems to be more subjective than 'threats' which could exist regardless of

subjective perceptions of international security actors. Etymologically, the word 'risk' originates from the ancient Greek word 'rhizikon' meaning 'a dangerous hazard'. In contemporary usage, risk refers to future uncertainty about a situation involving a degree of vulnerability to significant threats. In international security contexts, it implies any potential burden that international security actors are prepared to shoulder in order to realize their security objectives in the future. In this sense, risk involves any future uncertain and consequential activity about things that we consider valuable or important (Schrager, 2019; McChrystal and Butrico, 2021).

International security actors could cope with the future risks either through 'hedging' or 'risk acceptance'. When they choose hedging, which refers to a plan for minimizing the potential costs of the anticipated risks, they sacrifice some of their future gains in order to reduce the expected level of damage to their current acquired values. Therefore, hedging is preferred when the likelihood of the risk, and the impact of the damage, are expected to be very high. If the risky situation is expected to take place in a short period of time, this could also motivate international security actors to prefer hedging over accepting risks (Aven and Renn, 2010; Schrager, 2019; McKinsey & Company, 2023).

Alternatively, international security actors might also adopt 'risk acceptance' as a response to a low risk situation. In this case, they try to adopt themselves to the requirements of the risky situation without developing any hedging plan. This option is more preferable when the likelihood of the risk, and the impact of the damage, are expected to be low. If the risky situation is expected to take place in a longer period of time, this could also encourage the international security actors to choose the risk acceptance as a response to the risky situation (Aven and Renn, 2010; Schrager, 2019; McKinsey & Company, 2023).

It should be noted that the principles of risk management in international security differ significantly from those of risk management principles in the fields of economy and finance. The preferences of international security actors to hedge or accept specific security risks depend largely on their role as 'security-maximizers' in an environment usually characterized by actual and potential conflicts. By contrast, business actors could tend to be 'risk-takers' in their own business environment, which is sometimes characterized by actual or potential profits. For most of the international security actors, a precautionary risk avoidance tendency prevails over a risk-taking inclination. Likewise, risk acceptance choices of international security actors could work only if and when destructive risk consequences are adequately controlled or kept at a manageable level.

B. DYNAMIC VS STATIC RISK ASSESSMENT MODELS FOR HEDGING AND RISK ACCEPTANCE DECISIONS

Usually, it is the static risk assessment models that result in poor strategies and strategic decisions about 'hedging' or 'risk acceptance' choices, because they take all factors other than the risky situation and the international security actor for granted, or they consider them static and unchanging. This static understanding also relies on an unrealistic assumption that all capabilities and relationships of the international security actor should be monitored, analysed, and protected against all of the potential risks without any prioritization among them. Instead of taking a future-oriented approach, such static risk assessment models also rely on earlier risk assessments, which may not be relevant anymore. More importantly, unexpected risks, with critical destructive potential, could always exist. These weaknesses of the static models necessitate the adoption of more dynamic risk assessment models (Jain, Nauck, Poppensieker, and White, 2020; McKinsey & Company, 2023).

Therefore, dynamic risk management is needed to take measures against such critical risks to significant vulnerabilities. In addition, a dynamic rather than a static risk management model could be more proactive than reactive. This dynamic model of risk management suggests a risk-based one emphasizing the mitigation of the most critical vulnerabilities rather than hedging every risk everywhere (Jain, Nauck, Poppensieker, and White, 2020). Likewise, international security environments do change dynamically, creating unexpectedly new inputs for the risk assessment decision-making process continuously. Therefore, it is always very important to expect the unexpected in the risk assessment process. These dynamic changes sometimes require us to revise or update our 'hedging' or 'risk acceptance' decisions continuously so that we can take new measures to mitigate emerging risks or we could revise our earlier hedging decision by accepting certain risks if we become more resilient against such risks (Vellani, 2020; McKinsey & Company, 2023).

This is the main reason why many actors update their risk assessment documents regularly. For example, NATO's documents in this respect include the NATO Military Strategy as well as the NATO Strategic Concept, which was recently updated at the NATO 2022 Madrid Summit (NATO, 2022). NATO Headquarters has been working through its specialized bodies in order to produce the most dynamic risk assessment of security risks. Among these bodies, the most important role is played by the Allied Command Transformation (ACT), which develops competitive and innovative strategies for NATO in order to enhance its warfighting capacity in a dynamically changing strategic context (NATO, 2023a). To this purpose, ACT publishes the Strategic Foresight Analysis (SFA), which regularly identifies possible scenarios by exploring the evolving security environment and its implications for NATO (NATO, 2024). There is also an Emerging Security Challenges Division (ESCD), which reviews NATO's non-traditional risks and challenges (NATO, 2023b). Similarly, the OECD (2022) produces its "Risks That Matter Survey" regularly in order to account for the critical risks to the developed economies of the world. Likewise, the European Union produces its own "Future Shocks", the most recent in 2023 (EPRS, IPOL, and EXPO, 2023). These publications include best practice examples of dynamic risk assessment models for managing international security risks, as they refrain from adopting a static

approach to the risk assessment process.

Since dynamic risk assessment and risk management processes require the contributions of all relevant actors at various degrees, the organizational framework for collecting and analysing information about risks should be flexible enough in order to avoid possible problems associated with the hierarchical organizational structures. This could be an important challenge for international security actors as they find it quite difficult to adopt more flexible and less hierarchical networking models. Therefore, effective risk assessment and management processes should include both bottom-up and top-down flow of information about the future risks as well as the adoption of risk mitigation and risk adaptation measures (Vellani, 2020; McKinsey & Company, 2023).

In this respect, a dynamic approach to risk management could offer more effective solutions to challenges of hedging or accepting international security risks. Regarding the hedging behaviour, the dynamic approach to risk management requires more accurate assessments of new threats and the identification of changes in existing threats as well as the vulnerabilities in the existing hedging solutions. Regarding the risk acceptance behaviour, this process also involves the determination of one's risk acceptance or risk-taking readiness against minor or not-so-critical risks everywhere (Jain, Nauck, Poppensieker, and White, 2020; McKinsey & Company, 2023). In fact, for all international security actors, there is no objective criteria for risk acceptance choices, since their risk-taking appetite depends on their own military capacity and sovereign preferences about their own security.

Generally, risks are assessed and prioritized by relating the potential impact of an event on the international security actor against the level of certainty about the impact. In this way, all risks could be ranked in terms of their relative prioritization. Since international security actors could cope with low-impact and high-likelihood risks in accordance with their existing guidelines, they focus more on the high-impact and low-likelihood risks in deciding whether these risks should be hedged or accepted. In their dynamic

risk assessments, international security actors also use probability ratings about the likelihood of security attacks. In such risk assessments, the history of earlier attacks as well as the existence of the capability to execute an attack, intent, and motivation are taken into consideration. Based on the risk assessment, the actual risk is determined in terms of the likelihood categories of very unlikely, unlikely, moderate, likely, and very likely (Aven and Renn, 2010; Schrager, 2019; Vellani, 2020).

Even if it is ultimately up to international security actors to make these assessments about the security risks, and to make strategic decisions about managing these international security risks, they usually follow common rational principles and models. Accordingly, a risk management process is implemented rationally in order to make well-informed decisions about balancing the cost of risk mitigation with the benefits of the desired security action. Therefore, it is not rational to seek risk elimination which is either too costly or unrealistic. Instead, the risk management process should enable the decision makers to reduce the expected uncertainty and damages in the future to a minimum level. It should also enable the decision makers to realize not only threats but also opportunities (Aven and Renn, 2010; Schrager, 2019; Vellani, 2020; McKinsey & Company, 2023).

Therefore, any effective risk management strategy could benefit from the well-known SWOT (Strength, Weakness, Opportunities, and Threats) analysis as well as situational awareness about the STEEP (Social, Technological, Environmental, Economic, and Political) analytical frameworks. These risk assessments about the resilience of international security actors and their wider strategic environment involve strategic decisions to be taken under uncertainty (Yoe, 2019; Fisher, Wisneski, and Bakker, 2020). In the following sections, the significance of employing the SWOT analysis as well as the STEEP analytical frameworks will be emphasized in terms of their role in strengthening the strategic security risk management capacity of international security actors about future warfare dynamics and strategic situational awareness across domains.

C. HEDGING AND RISK ACCEPTANCE RESPONSES TO THE CHALLENGES OF FUTURE WARFARE

Since all risks are expectations about the future, the risk assessments of international security actors originate from their expectations about and strategies for coping with the challenges of future warfare (Freedman, 2017). In doing so, they assume that future warfare is likely to create new opportunities and threats for their current or expected future strengths and weaknesses. Therefore, this type of risk assessment involves a SWOT analysis of their relationship to the expected characteristics of future warfare, in which high precision weapons with greater lethality are expected to play a more decisive role in bringing about military victory. Consequently, risk assessments about future warfare as well as the accompanying hedging and risk acceptance solutions tend to assume that future wars will be under the control of those international security actors with greater technological superiority against their rivals (Rasmussen, 2006; Heng, 2006).

The introduction of new technologies in future wars is also expected to result in a "Revolution in Military Affairs" (Metz and Kievit, 1994; Freedman, 2017). The supporters of this view assert that the advances in military technology reduce or even eliminate the risks in future warfare for those international security actors that have greater access to the new military technologies. They also suggest that these technological developments will necessitate that militaries transform themselves into a smaller, more mobile, and more competent organization. The technology-based views of future warfare also note that future wars should be waged with cheaper economic costs, and minimum human casualties, as these could be more targeted and controlled wars. They also emphasize the importance of a greater use of digital technologies, artificial intelligence, networked communications, satellite-based surveillance, robot-process automation, unmanned drones, hypersonic rockets, precision weapons, and other disruptive military technologies (Mandeles, 2005).

Although technological superiority is one of the most important aspects of military power, non-technological aspects of warfare still remain crucial factors in shaping the outcomes of future wars. Actually, the assumption that those actors with these new technologies could prevail over the others who have limited or no access to the new technologies may result in over-emphasis on technological superiority and underestimating other possible risks related to the non-technological challenges of future warfare. In fact, the space-technology-assisted surveillance technologies as well as more precise weapon systems may not guarantee the complete defeat of enemies with less technological armies since they might use some of the conventional weapon systems and unconventional war tactics more disruptively (Matt, 2023; Watling, 2023).

Therefore, future wars with sophisticated technologies could create diverse opportunities and threats as well as hedging and risk acceptance options for international security actors depending on their military and non-military strengths and weaknesses. Accordingly, major military powers with sophisticated weapons technologies may find it too risky to attack each other due to the balance of terror, created by the annihilatory power of nuclear and other weapons of mass destruction (WMD). Ironically, increasing risks of nuclear warfare in the form of "total war" without an option of differentiating between civilians and soldiers could make non-nuclear military strategies more relevant options for future warfare scenarios (Dunay, 2023; 7-11).

Another serious risk about future warfare seems to be the humanitarian challenges associated with the weakening role of morality, politics and diplomacy. Warring sides and their proxies could ignore important humanitarian aspects of warfare when they engage in armed conflicts by not prioritizing morality, not clarifying war objectives and not minimizing the lethality of their weapon systems in future wars (Virilio, 1997; Coker, 2004). Russia's ongoing war crimes during its war against Ukraine, which started in 2014 but intensified after 2022, could be considered as an example of serious humanitarian risks for future wars.

In addition, in various parts of the world with specific warfare conditions, as in Africa or Asia, conventional weapon systems and unconventional war tactics are still used disruptively. The warring sides in these parts of the world usually lack high-tech armies or sophisticated weapons systems. In such contexts of future warfare, non-technological security risk factors could be prioritized over technology-based security risk assessments. In such future warfare contexts, the risks of unconventional wars, proxy wars and hybrid wars could characterize security risk management strategies more than technology-based security risks (Kaldor, 1999). Accordingly, a greater hybridization of warfare could emerge as another important strategic risk of future warfare. This could also increase the severity of hybrid risks such as cyber-attacks and the weaponization of trade, energy, migration, logistical supply of critical resources, and other transnational socio-economic activities (Najzer, 2020).

Not surprisingly, in the hybrid contexts of future warfare, the emerging dynamics and characteristics of warfare could reduce predictability and increase uncertainty, since hybrid and asymmetric conflicts could create even more critical security risks for many international security actors. Similarly, the introduction of more artificial intelligence and robotic weapon systems could also create even more disruptive and unpredictable conditions for all international security actors at the national, regional, international, and global levels of future warfare (Coker, 2004; Najzer, 2020).

To sum up, dynamic responses to the challenges of security risk management and the adoption of effective hedging and risk acceptance solutions necessitate greater emphasis on disruptive capabilities, which could be linked to technological or non-technological aspects of future warfare. This is connected to the fact that it is almost impossible to predict and control how enemies could respond to new military technologies as well as to strategies. Future warfare is likely to continue to be unpredictable and an inherently uncertain human activity. Despite the existence of sophisticated war technologies and strategies, warfare is likely to remain an essentially uncertain conflict with diverse possibilities and critical risks, which could be managed effectively only through a dynamic, strategic approach rather than a static, inflexible one.

D. MANAGING SECURITY RISKS IN THE COMPLEX STRATEGIC ENVIRONMENT OF FUTURE CROSS-DOMAIN WARFARE

A dynamic and strategic approach is also necessary for managing international security risks in the complex strategic environment of future cross-domain warfare across land, maritime, air, space, and cyberspace. Therefore, international security risk assessments need to pay attention to developments in various domains of military activity as well as their interactions among themselves. As present wars tend to take place across various domains, future wars could require a greater integration of physical and cyber domains, thus necessitating weapon systems in various platforms through advanced satellite-based communication technologies (Alberts, Garstka, and Stein, 2000).

To make better risk assessments and to adopt effective international security risk management strategies regarding hedging and risk acceptance options, comprehensive contextual analysis across domains could be very helpful in enhancing strategic situational analysis for all international security actors involved. In this respect, the STEEP could offer such an analytical tool for exploring the impact of the developments in the Social, Technological, Economic, Environmental and Political contexts on the military capacity of any international security actor (Kuznar, 2023). This analysis could enable security risk analysts to study risks related to historical experiences, socio-cultural values and political orientations, as well

as technological and environmental conditions of international security actors and their security alliances, which could be considered as actors belonging to international security communities (Adler and Barnett, 1998).

The STEEP analysis enables international security risk analysts to incorporate the previously neglected environmental dynamics into their assessment of future warfare across all domains. In addition to well-known socio-economic and political factors, such as migration trends, trade disruptions and political instabilities, climate change also emerges as a key environmental challenge which shapes the effectiveness of international security risk management strategies considerably. For example, the latest Strategic Foresight Analysis of NATO ACT highlights the inability of weaker states to mitigate the impact of extreme climate disruptions as a security risk since this could increasingly make such states more fragile or cause an even more threatening security risk of state collapse (NATO, 2024: 25).

Within the STEEP analysis, technological context is defined by its interactions with the political, socio-economic, and environmental contexts across all domains of military activity. Therefore, the risk management decisions about hedging and risk acceptance options would certainly involve choices not only about the use of technological weapons systems but also their socio-economic, political, and environmental implications for these domains. To this purpose, it is important to employ a broader and more inclusive approach to security risk analysis, covering economic, socio-political, psychological, and environmental dimensions, in addition to the conventional military dimension. Actually, with the widening and deepening of the security conception, all social, technological, environmental, economic, and political manifestations of the security risks could be analysed more systematically across domains in national, regional, international, and global contexts (Krause and Williams, 1996: 229-254; Buzan and Waever, 1998). Such a comprehensive approach to security risk analysis could be quite useful since there has also been a tendency to integrate these five domains for future military operations.

At this point, it is important to clarify the difference between the above-mentioned narrower concept of military operational domains, including land, maritime, air, space, as well as cyberspace, and the broader concept of multi-domain operations, which is beyond the scope of this paper. According to NATO (2023c), Multi-Domain Operations (MDO) denotes the harmonization of military activities across all operating domains and environments with the non-military activities of external stakeholders in order to create unfavourable conditions for the adversaries.

At present, only a few international security actors and alliances are able to integrate their activities across all operational domains (Bronk and Cranny-Evans, 2022). Nevertheless, a considerable number of international security actors are able to integrate, at minimum, their land, air, and cyberspace domains. With the advances in their technology, more international security actors are expected to integrate most of their domains more effectively. In fact, the use of drones with artificial intelligence, surveillance techniques, and high-precision weapons contributes to the spread of cross-domain integration capacity to a greater number of international security actors around the world at more affordable costs (Wang, Li and Leung, 2015: 1379–91).

As a result of the tendency to integrate existing domains of military activity, international security actors tend to develop their own network-centric strategies of warfare. The availability of new weapons systems with developed sensors and high-precision weapons enables them to become more networked and integrate their capabilities of detecting, targeting, and destroying enemies. In this respect, and among many other factors, the integration of four main factors (i.e. arms, sustainment, societal capacity, and communications) seems to be driving the evolution of future warfare across domains. The developments in these areas could change the tactics used and increase the agility and complexity of employing military force in increasingly networked future warfare across domains further. Similarly, the developments in communications technology could also make electronic warfare with sophisticated radars and sensors very effective due to the synchronization of operational theatres through communication channels. Therefore, the capacities of international security actors to achieve cross-domain integration will be decisive factors in shaping their international security risk

management choices regarding future warfare conditions (Alberts, Garstka, and Stein, 2000; Watling, 2023).

In future warfare, the cross-domain integration and increasing interconnectedness among the military units will create both positive and negative conditions for risk aggregation and effective security risk management across domains for the social, technological, economic, environmental and political contexts. In fact, cross-domain integration could contribute positively to the enhanced strategic situational awareness of international security actors at these dimensions of security, since they could understand their position, strengths, and weaknesses vis-à-vis friends and foes individually and collectively better with the help of cross-domain integration. Consequently, any international security actor could define its hedging and risk acceptance options more strategically and have a clear competitive advantage over its rivals if it develops a better strategic situational awareness in the social, technological, economic, environmental and political contexts than its adversaries (Downes and Kwinn Jr., 2009).

Conversely, a greater integration tendency across domains could increase the risk of over-centralization. The neglect of this risk of over-centralization could create a critical security vulnerability for international security actors. Actually, when international security actors become too centralized, the more flexible, agile and speedy enemies could threaten them more easily and dangerously (Alberts, Garstka, and Stein, 2000; Watling, 2023). In order to cope with such uncertainties stemming from too much centralization in cross-domain integration and command structures, international security actors should promote the flexibility and training of their forces by delegating more decision-making capacity to such units. With more flexibility, training, and decision-making capacity, the military units could respond to unexpected threats more effectively and confidently in the social, technological, economic, environmental and political contexts of future warfare across domains (Freedman, 2022; Watling, 2023).

To summarize, international security actors and their alliances could cope with the challenges of future cross-domain integration by creating more flexible organizational structures, enhancing the agility of the military units, and strengthening the operational and technological resilience of these military units within the wider social, technological, economic, environmental and political contexts of military activity.

E. RECOMMENDATIONS FOR NATO

It could be stated that compared to other military alliances in human history, NATO has been the most successful one in updating its strategic assessments regularly with a forward-thinking perspective so that major risks are managed more systematically and key hedging and risk acceptance options are defined more strategically (Monaghan, 2022; Dunay and Rhodes, 2022: 7-9). The following actionable recommendations could further enhance NATO's existing resilience, agility, and strategic superiority vis-à-vis its adversaries.

First, ACT and ESCD, which already play important roles in NATO's risk management processes, could communicate their most important risk management solutions to all relevant NATO units at the strategic, operational and tactical levels interactively. To this purpose, both ACT and ESCD may create a communication channel through which all NATO units could be informed about NATO's updated risk management solutions as well as its hedging and risk acceptance preferences regularly and share their feedbacks with ACT and ESCD swiftly. In addition, the ACT and ESCD could also create specialized units for the strategic communication of NATO's risk management approach to NATO's key stakeholders in the global strategic environment.

Second, NATO could coordinate its existing digitalization and international security risk management processes more closely. This coordination will enhance NATO's security risk analysis capacity through benefiting from its increasingly more sophisticated digitalized information management system. This could strengthen NATO's capacity to employ both the SWOT and the STEEP analytical frameworks since these risk analysis methods require a greater use of data and digital capacity for producing comprehensive international security risk assessments. In this respect, mixed quantitative and qualitative methodologies could be employed for processing multiple forms of information systematically.

Third, NATO could promote an even more resilient, agile and flexible organizational culture and structure to enhance innovative problem-solving capabilities throughout the Alliance at all levels so that they can counter potential threats as forcefully and swiftly as possible. In this way, NATO could strengthen its organizational culture and identity as a "shared risks security community" which identifies common security risks and finds common solutions to these security risks collectively. Accordingly, the Alliance could focus on shaping the future world of their choosing proactively, rather than simply responding reactively to threats created by their rivals. This dynamic strategic vision for rebuilding NATO as a "shared risks security community" could not only bring its members with diverse interests, identities and orientations closer to one another, but also transform the already very strong NATO Alliance into an even more proactive, resilient, and agile security organization.

CONCLUSION

The key findings of this research paper suggest that the way in which international security actors, as well as security alliances such as NATO, hedge or accept future international security risks could be critical for the success of their international security risk management strategies. The paper suggests that the adoption of a dynamic and strategic approach to future security risks could play a crucial role in making security risk management strategies more proactive, resilient, and agile under the hybrid conditions of anticipated warfare across-domains.

In this respect, a dynamic rather than a static approach to international security risk management requires the adoption of a 360-degree approach as well as a systematic collection and analysis of data about emerging security risks. The adoption of such an information-based rather than a threat-centric security risk management strategy involves taking a multi-disciplinary approach to international security risk management process. To this purpose, the findings of the academic disciplines of military science and international relations could be harnessed to other social science disciplines of political science, public administration, business administration, finance, and actuarial science so that security risk assessments and processes could reflect a richer knowledge base and a more comprehensive and inclusive strategic vision for security risk management.

All in all, the dynamic and strategic approach to international security risks necessitates the adoption of either hedging solutions in prioritized strategic areas where vital interests are threatened or risk acceptance solutions in other inconsequential areas where certain security risks could be accepted and tolerated. Therefore, a well-planned international security risk management strategy with appropriate decisions to hedge and accept risks could serve as both an effective deterrent and a strategic asset in future warfare contexts across domains.

REFERENCES

Adler, E. and M. Barnett, (1998) “A Framework for the Study of Security Communities”, in E. Adler, and M. Barnett (eds), Security Communities, Cambridge University Press.

Alberts, D.S., J.J. Garstka, F.P. Stein (2000) Network Centric Warfare: Developing and Leveraging Information Superiority, 2nd Ed. US DoD C4ISR Cooperative Research Program, CCRS.

Aven T. and O. Renn (2010), Risk Management and Governance: Concepts, Guidelines and Applications, Springer.

Bronk J. and S. Cranny-Evans, (2022) ‘Building the Capacity to Conduct Joint All-Domain Operations (JADO): Considerations for the UK’, RUSI Occasional Papers, November. Retrieved https://static.rusi.org/345_OP_JADO.pdf

Buzan, B. and O. Waever, (1998), Security: A New Framework for Analysis, Lynne Rienner Publishers.

Coker C. (2004) The Future of War: The Re-Enchantment of War in the Twenty-First Century, Wiley-Blackwell.

Clark, B. D. Patt and H. Schramm, (2020), ‘Mosaic Warfare: Exploiting Artificial Intelligence and Autonomous Systems to Implement Decision-Centric Operations’, CSBA. Retrieved https://csbaonline.org/uploads/documents/Mosaic_Warfare.pdf.

Downes P. and M. J Kwinn Jr, (2009), ‘Proving Situational Awareness Impact in the Land Warrior Project’, Military Operations Research, Vol. 14, No. 4, pp. 47–59.

Dunay, P. and M. Rhodes (2022) Challenges Ahead: NATO Prepares for the 2030s and Beyond, per Concordiam: Journal of European Security and Defense Issues, Vol.12, No.2. pp. 7-9.

Dunay, D. (2023) Risky But Manageable: Strategic Deterrence in the Nuclear Era, per Concordiam: Journal of European Security and Defense Issues, Vol.12, No.3. pp. 7-11.

Eriksson, Johan (ed.), (2001), Threat Politics: New Perspectives on Security, Risk and Crisis Management, Ashgate.

EPRS (European Parliamentary Research Service) with the EU DG for IPOL (Internal Polices) and EXPO (External Policies) (2023), Future Shocks 2023: Anticipating and Weathering the Next Storms, July. Retrieved https://www.europarl.europa.eu/RegData/etudes/STUD/2023/751428/EPRS_STU(2023)751428_EN.pdf

Fisher, G., J.E. Wisneski, and R.M. Bakker, (2020) Strategy in 3D: Essential Tools to Diagnose, Decide, and Deliver, Oxford University Press.

Freedman, L. (2017) The Future of War: A History, PublicAffairs/Hachette Book Group.

Freedman, L. (2022) Command: The Politics of Military Operations from Korea to Ukraine, Allen Lane.

Heng, Y., (2006), War as Risk Management: Strategy and Conflict in an Age of Globalised Risks, Routledge.

Jain, R., F. Nauck, T. Poppensieker, and O. White, (2020) Meeting the Future: Dynamic Risk Management for Uncertain Times, August. Retrieved https://www.mckinsey.com/~/media/mckinsey/business%20functions/risk/our%20insights/meeting%20the%20future%20dynamic%20risk%20management%20for%20uncertain%20times/meeting-the-future-dynamic-risk-management-for-uncertain-times.pdf

Jervis, R., (1978) “Cooperation under the Security Dilemma”, World Politics, Vol. 30, No. 2, pp.167-214.

Jervis, R., (1985) “Perceiving and Coping with Threat”, in R. Jervis, R. N. Lebow and J. G. Stein (eds), Psychology and Deterrence, The Johns Hopkins University Press.

Kaldor, M. (1999) New and Old Wars, Polity Press.

Krause, K. and M. C. Williams, (1996) “Broadening the Agenda of Security Studies: Politics and Methods”, Mershon International Studies Review, Vol.40, No. 2, pp.229-254.

Kuznar, L.A., (2023) 21st Century Information Environment Trends out to 2040: The Challenges and Opportunities in the Integration of Its Physical, Cognitive, and Virtual Domains, Open Publications, Vol.8, No.1.

Mandeles, M. (2005) The Future of War: Organizations as Weapons, Potomac Books.

Matt, C., (2023) Strategic Aspects of Digital Transformation for Military Organisations, Open Publications, Vol.8, No.3.

McChrystal, S. A., A. Butrico, (2021) Risk : A User’s Guide, Portfolio/Penguin,.

Metz, S. and J. Kievit, (1994) The Revolution in Military Affairs and Conflict Short of War. US Army War College Press.

Monaghan S, (2022) Resetting NATO’s Defense and Deterrence: The Sword and the Shield Redux, CSIS Brief, June. Retrieved https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/220628_Monaghan_ResettingNATO_DefenseDeterrence.pdf?VersionId=j73cwvXqZmuKo5VBYY.xPMp3Z7X2y7Yx

NATO (2022) NATO 2022 Strategic Concept. Retrieved https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf

NATO (2023a) Allied Command Transformation. Retrieved https://www.nato.int/cps/en/natohq/topics_52092.htm

NATO (2023b) Emerging Security Challenges Division (ESCD). Retrieved https://esc.hq.nato.int/default.aspx

NATO (2023c) Multi-Domain Operations in NATO – Explained. Retrieved https://www.act.nato.int/article/mdo-in-nato-explained/

NATO (2024) “Allied Command Transformation Strategic Foresight Analysis 2023”, Retrieved https://www.act.nato.int/wp-content/uploads/2024/01/SFA2023_Final.pdf

Najzer, B. (2020) The Hybrid Age: International Security in the Era of Hybrid Warfare, I.B. Tauris

OECD (2022) The OECD Risks That Matter Survey Retrieved https://www.oecd.org/social/risks-that-matter.htm#publications

Rasmussen, M. V. (2006) The Risk Society at War, Cambridge University Press.

Schrager A. (2019) An Economist Walks into a Brothel and Other Interesting Places to Understand Risk, Portfolio/Penguin.

Vellani K.H., (2020), Strategic Security Management A Risk Assessment Guide for Decision Makers, 2nd Edition CRC Press/Taylor & Francis Group.

Virilio, P. and Lotringer, S. (1997). Pure War (M. Polizotti, Trans.). New York: Semiotext(e).

Wang, X. Li X. and Leung, V. C. M. (2015) ‘Artificial Intelligence-Based Techniques for Emerging Heterogeneous Network: State of the Arts, Opportunities, and Challenges’, IEEE Access, Vol. 3, pp.1379-91. Retrieved https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7185326

Watling J., (2023) Supporting Command and Control for Land Forces on a Data-Rich Battlefield, RUSI Occasional Paper, July.

Retrieved https://static.rusi.org/Supporting-command-and-control-for-land-forces-on-a-data-rich-battlefield.pdf

Wolfers, A. (1962) ‘National Security as an Ambiguous Symbol’, in Discord and Collaboration. Essays on International Politics John Hopkins University Press, pp. 147-165.

Yoe, C. (2019). Principles of Risk Analysis: Decision Making Under Uncertainty, CRC Press.

McKinsey & Company, (2023) What is business risk? McKinsey Explainers, August Retrieved https://www.mckinsey.com/~/media/mckinsey/featured%20insights/mckinsey%20explainers/what%20is%20business%20risk/what-is-business-risk.pdf

Risk Acceptance in Future Warfare across Domains
www.openpublications.org